MASTER EN SCIENCES INFORMATIQUES

Concept du guichet unique: application à AdmiPRO-PBFlow

Frankinet, Philippe

Award date:
2001

FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX, NAMUR

INSTITUT D'INFORMATIQUE

RUE GRANDGAGNAGE, 21, B-5000 NAMUR (BELGIUM)

Concept du guichet unique : application à AdmiPRO - PBFlow

Philippe Frankinet

Mémoire présenté en vue de l'obtention du grade de
Licencié en Informatique

Année Académique 2000 - 2001

RESUME

Ce document traite du concept du guichet unique et de son application dans les administrations européennes. Un cas pratique sera abordé afin d'illustrer le concept et son intégration dans les organisations.

Ce travail se découpe en quatre parties. Dans la première, le concept du guichet unique est explicité et une typologie est alors réalisée. On relate les diverses expériences dans les pays européens. Un cas pratique est développé en détail dans la seconde partie. Dans la troisième partie, le problème de la représentation de l'organisation est décrit. La problématique de la signature électronique des documents et des mécanismes de preuves terminent ce travail. Le cas pratique abordé dans la seconde partie sert de base pour le développement des solutions à ces deux problèmes.

mots clés: guichet unique, one stop government, AdmiPRO, PBFlow, annuaire électronique, signature électronique

ABSTRACT

This paper deals with the concept of single window and his application into european public administration. A case study will be described to illustrate this concept and his integration into organisations.

This works follows a four step approach. The first step explains the concept of single window and a typology is made. Several european case studies are described. A practical case is developped in detail in the second step. In the third step, organizational representation is described. Digital signature and the problem of proof end this work. The pratical case will show how to build solutions related to these two problems.

keywords: single window system, one stop government, AdmiPRO, PBFlow, directory service, digital signature

AVANT-PROPOS

Je tiens à remercier:

Madame Claire Lobet-Maris, promoteur de ce mémoire, pour sa disponibilité, ses critiques judicieuses et ses conseils durant toutes les étapes de ce travail;

Messieurs William Poos et Massimo Marmoro pour leur aide et leurs suggestions avisées;

La direction de NSI sa pour sa collaboration, et en particulier monsieur Philippe Oeyen;

Ma famille, collègues et amis, qui par leurs encouragements et leur patience, m'ont permis d'aller jusqu'au terme de ces trois années d'études;

Toutes les personnes qui de près ou de loin m'ont aidé à réaliser ce travail.

Je remercie les membres du Jury de l'intérêt qu'ils voudront bien porter à la lecture de ce travail.

TABLE DES MATIERES

TABLES DES FIGURES

GLOSSAIRE

Applet : Element graphique Java pouvant être incorporé à une page Web.

Autorité de certification : Organisme ou société privée fournissant des certificats électroniques.

ACL : Access Control List . Mécanisme définissant les droits d'accès à une ressource.

ASN.1 : Abstract Syntax Notation 1

AdmiPro : Plate-forme administrative développée par NSI s.a. et basée sur l'expérience du projet PBFlow.

B2B : Business to business. Se dit d'un système mettant en relation clients et fournisseurs. La particularité de ce système est que le client est une société, elle même pouvant être un fournisseur d'autres produits.

CA : Certificate Authority. Voir autorité de certification.

CCITT : Consultative Committee on International Telephony and Telegraphy.

COST A14 : "COST A14, Government and Democracy in the information Age". Acronyme pour "Coopération internationale dans le domaine scientifique et technologique". Il s'agit d'un groupe de travail dépendant du conseil de l'Europe.

Cryptogramme : Texte ou contenu chiffré.

Cryptosystème : procédé de transformation en cryptographie.

DAP : Directory Access Protocol. Protocole utilisé pour accéder aux services X500.

DIT : Directory Information Tree. Structure hiérarchique formant la structure de base d'un annuaire électronique.

FAQ : Frequenly Ask Question. Se dit d'un fichier, ou l'équivalent, reprenant les questions (et forcément les réponses) les plus fréquemment posées sur un sujet déterminé.

GED : Gestion électronique des dossiers

Guichet unique : Mode de prestation visant à regrouper des services administratifs, ou des renseignements à leurs sujets, afin que le citoyen consacre moins de temps et d'efforts pour trouver et obtenir ce qu'il recherche.

HTTP : Hyper Text Transfert Protocol. Protocol utilisé sur Internet, entre autre pour le transfert de page Web.

IETF : Internet Engineering Task Force. Organisme définissant des standards Internet sous la forme de documents appelés RFC (Request for Comments). Une fois les documents RFC approuvés, ils deviennent des standards.

Java : Langage de développement mis au point par Sun Micrsosystems. Il s'agit d'un langage orienté objet dont la principale caractéristique est sa portabilité garantie grâce à l'utilisation d'une machine virtuelle pour son exécution.

JNDI : Java Native Directory Interface. Cette librairie Java fournit une manière standardisée d'accéder aux services de noms. Les fonctionnalités particulières des services de noms, comme par exemple LDAP ou DNS, sont fournies par des librairies annexes.

JUnivers : Couche logicielle Java de NSI s.a. qui fournit une série d'outils permettant de réaliser et de déployer rapidement une application Java.

LDAP : Lightweight Directory Access Protocol. Développé afin d'alléger le protocole DAP, il est utilisé pour accéder aux annuaires électroniques.

Legal XML : Extension du standard XML appliqué au domaine judiciaire.

NSI : Nouvelles Solutions Informatiques. Prestataire informatique liégeois ayant réalisé le logiciel AdmiPRO (http://www.nsi-sa.be).

OSG : One Stop Government. Voir guichet unique.

One Stop Government : Voir guichet unique.

OSI : Open Systems Interconnect. Système en 7 couches résultant des efforts du CCITT afin de définir un système pour le transport des données, allant du transport physique des données aux protocoles applicatifs.

Passphrase : mot de passe permettant de lire une clé privée.

PBFlow : Projet développé en 1996 par l'université de Namur, la Région Wallonne et les autorités communales de la ville de Namur mettant en place un guichet unique dédié à l'octroi des permis de bâtir.

PKCS : Public Key Cryptography Standard. Standard utilisé dans la cryptographie à clé publique définissant entre autres les formats des certificats électroniques.

PKI : Public Key Infrastructure. Système d'infrastructure à clé publique. Il s'agit d'un système basé sur les systèmes asymétriques de cryptographie, permettant la distribution et le stockage de clés électroniques utilisées pour le cryptage, l'authentification et la signature électronique.

Repository : Système contenant une collection d'informations.

RFC : Request for Comments. Document définissant un futur standard Internet.

SASL : Simple Authentification and Security Layer. Mécanisme standardisé d'authentification.

Servlet : Element Java permettant de traiter des requêtes Internet émise via HTTP.

Single Window : Terme anglais signifiant « guichet unique ».

Smart Card : Système de carte à puce permettant de stocker des certificats à clé privée - clé publique.

SSL : Secure Socket Layer. Protocole sécurisé de communication utilisant les certificats électroniques.

Workflow : Système de modélisation de procédures.

X500 : Service d'annuaire créé en 1988 par le CCITT.

X509 : Format hérité de X500 définissant les certificats électroniques.

XML : eXtensible Markup Language. Langage structuré permettant de définir la structure et le contenu d'un document électronique.

INTRODUCTION

L'objectif de ce travail est d'étudier le concept des guichets uniques et leurs applications dans les administrations européennes, et plus particulièrement belges. Les guichets uniques seront différenciés selon leurs particularités et on s'attachera particulièrement à décrire certains facteurs rencontrés lors de la mise en place d'un tel système.

Le travail vise à la compréhension des problèmes posés, à l'aptitude à faire une synthèse de la veille technologique effectuée et à l'apport de solutions originales et personnelles. Pour des raisons évidentes de confidentialité que le lecteur comprendra aisément, certaines parties des solutions ne seront pas dévoilées. C'est le cas, entre autre, du code développé.

La démarche de ce travail se structure en quatre parties, à savoir :

1ère partie : L'étude du concept
2ème partie : Un cas pratique abordé en détails
3ème partie : Problématique de la représentation organisationnelle
4ème partie : Problématique de la signature électronique et des mécanismes de preuve

Le premier chapitre est consacré à l'étude du concept du guichet unique et à la réalisation d'une typologie. Afin d'aider le lecteur dans la compréhension de ce concept et de la typologie, quelques exemples européens seront décrits.

Le deuxième chapitre porte sur la description détaillée d'un guichet unique belge. Le contexte et les objectifs visés par ce guichet unique sont abordés. On décrit de façon précise les aspects fonctionnels pour terminer sur les facteurs étudiés par la suite.

Le troisième chapitre est consacré à la problématique de la représentation organisationnelle. Les systèmes de représentation organisationnelle sont présentés et on décrit la solution mise en place dans l'exemple développé au deuxième chapitre

La quatrième chapitre traite du problème des signatures électroniques et des mécanismes de preuves. La cadre légal est abordé au travers des directives européennes et leurs transcriptions dans le droit belge. Une solution technique est détaillée et illustrée par l'exemple repris au deuxième chapitre.

Le travail se termine sur les quelques problèmes non abordés ici et sur les perspectives futures de tels systèmes.

Chapitre 1 One Stop Government

Ce chapitre introduit le contexte des réformes administratives et le concept du "One Stop Government". Une fois les critères de classification abordés et la typologie présentée, quelques exemples des diverses approches nationales sont décrites.

1.1 Contexte général des réformes administratives

1.1.1 Contexte général

Les services publics ont tendance à faire évoluer leurs prestations de services. Différents éléments viennent justifier ce fait mais deux d'entre eux retiennent l'attention, à savoir les éléments liés à l'amélioration de la qualité du service offert au citoyen, et ceux qui sont liés à l'évolution des technologies de l'information.

Diverses réflexions ont été menées sur l'amélioration de la qualité du service offert au citoyen. Une de ces réflexions, la légitimité des administrations et les exigences des citoyens, mérite une attention toute particulière. D'un côté, on observe une administration publique rigide mais qui garantit un traitement équitable entre citoyens, et de l'autre, les entreprises privées soumises à la concurrence mais qui possèdent une certaine souplesse de fonctionnement et de développement.

1.1.2 Les attentes du citoyen et du secteur privé

Comme le souligne le Dr Claire Lobet-Maris[1], « *il faut pouvoir opposer les droits des citoyens sur leur administration ... ceux-ci cessent d'être respectés quand les lenteurs administratives, la complexité des procédures, les défauts d'information ne permettent plus aux citoyens d'exercer leurs droits dans des délais respectables* » .

Bon nombre de citoyens ont déjà été confrontés à l'administration, que ce soit pour des problèmes d'accessibilité, pour la multitude de documents à fournir ou encore pour les délais du service. Le citoyen a donc du mal à accepter certaines lourdeurs de l'administration publique alors qu'il est traité de manière très différente par les entreprises privées. Ce constat est renforcé par les conclusions d'une étude européenne[2] dans le cadre du réseau COST A14 dont quelques pages parlent des demandes des citoyens, qui seraient les suivantes :

- éviter l'interaction avec l'administration le plus souvent possible;
- obtenir un service rapide, c'est-à-dire supprimer les files d'attentes et résoudre le plus rapidement possible le problème rencontré;
- accéder de manière aisée aux différents services, c'est-à-dire accéder aux services à des heures convenant à la vie actuelle et si possible sans effectuer de grands déplacements;
- obtenir une information compréhensible par tous et qui demande peu d'efforts de la part de l'administré.

On peut constater que pour la plupart des citoyens, l'administration telle qu'elle est perçue ne remplit plus son rôle, soit parce qu'elle n'a pas évolué ou soit parce qu'elle a mal

[1] Lobet-Maris C., 2001, p.5
[2] Hagen M, Kubicek H., 1999, p.4

évolué. Ce sentiment est renforcé par le fait que ces mêmes citoyens constatent une évolution plus rapide des services dans le monde privé.

Cette étude en vient à la conclusion qu'un modèle organisationnel adéquat est nécessaire afin que l'administration s'adapte à la vie actuelle, mais aussi que les prestations de services doivent être réalisées selon les perspectives des citoyens[3].

Le secteur privé rencontre des problèmes similaires, comme des procédures longues et complexes. Elles attendent donc aussi une amélioration des services administratifs afin de consacrer moins de ressources, humaines et financières, aux relations qu'elles entretiennent avec l'administration.

1.1.3 L'informatisation des services publics

Outre l'adaptation des prestations de services, les services publiques doivent faire face à l'évolution toujours plus rapide des technologies de l'information. Cela est d'autant plus vrai que le citoyen mesure le fossé grandissant entre entreprise publique et entreprise privée.

L'informatisation des administrations est un processus assez lent et jalonné de plusieurs étapes. Cette structuration est d'ailleurs reprise par le Dr Claire Lobet-Maris[4] commentant les résultats de l'étude européenne.

La première ***étape*** est dite ***industrielle*** car elle concerne la productivité des traitements. Les tâches simples et routinières mais dont le volume est important sont automatisées.

La seconde ***étape*** est dite ***opérationnelle***. Elle concerne la productivité des postes qui est améliorée au travers de la diminution des intermédiaires dans la chaîne des traitements et par le support de programmes informatiques directement utilisés au niveau des postes opérationnels.

L'***étape informationnelle*** agit directement sur la productivité de l'organisation. On n'agit pas seulement sur les opérations et les postes de travail mais aussi sur la coordination de ceux-ci. Le ou les systèmes d'informations de l'organisation se veulent cohérents et on parle d'intégration horizontale des postes et des services.

La dernière ***étape***, dite ***environnementale***, concerne la coordination de l'organisation avec son environnement. Il s'agit avant tout de simplifier les procédures de transaction et d'améliorer l'accès à l'information ainsi que la rapidité du service.

1.1.4 Les besoins en gestion électronique des traitements et des dossiers

Les demandes des citoyens (ou de l'administration publique) se traduisent généralement par l'ouverture d'un dossier et la réalisation d'une procédure, procédure

[3] Hagen M, Kubicek H., 1999, p.5
[4] Lobet-Maris C., 2001, p.9-11

souvent constituée d'une suite de tâches dont l'enchaînement est connu. Cette manière de voir les procédures administratives permet en effet de modéliser ces dernières lors des différentes étapes de l'informatisation. La gestion électronique des dossiers et des traitements et la circulation des informations deviennent alors importants.

La gestion des dossiers est aussi un élément important. Cette gestion des dossiers permet la consultation de ceux-ci, mais aussi une semi-automatisation ou automatisation complète de la production des documents ainsi que l'archivage de ces derniers.

Ces deux éléments, gestion électronique des traitements et des dossiers, sont complémentaires. La mise en place de la gestion électronique des dossiers s'intègre parfaitement à la standardisation et la formalisation des traitements, c'est-à-dire à une découpe des traitements en étapes logiques dont on peut déterminer les compétences et les outils nécessaires à leurs réalisations.

Une telle découpe des traitements permet un suivi d'avancement, ce qui constitue un plus car il est facile de déterminer exactement à quelle étape se trouve le dossier administratif. L'avertissement des dépassements des délais et l'échange des informations, tant au sein d'une administration mais aussi entre administrations, citoyens et secteur privé, complètent la gestion électronique des dossiers

Ce besoin en gestion électronique s'inscrit bien dans les réformes et l'informatisation des administrations. Il rencontre également le besoin de transparence vis-à-vis des administrés tout en ayant des exigences accrues au niveau de la productivité. Il permet aussi une modernisation des outils tout en garantissant confidentialité et intégrité des informations.

1.2 Le guichet unique

1.2.1 Concept du guichet unique

Tout le monde en convient, les administrations doivent adapter les modes de prestation des services en fonction des demandes des citoyens sans négliger pour autant leurs propres besoins. Il s'agit d'une conception plus interactive et personnalisée du service fourni au citoyen, dont la demande devient l'élément central du système.

Les guichets uniques, appelés aussi « One Stop Governement » ou plus généralement « Single Window », permettent cette approche. Il est difficile de définir avec précision ce concept, mais Bent S., Kernaghan K. et Marson Br. ont avancé la définition suivante :

« Essentiellement, ce mode consiste à regrouper des services gouvernementaux, ou des renseignements à leur sujet, de sorte que les citoyens consacrent moins de temps et d'efforts pour trouver et obtenir les services qu'ils cherchent. »[5] .

1.2.2 Définition des critères de base

Afin d'approcher plus finement le concept de guichet unique, nous proposons dans la suite de ce texte, et en nous appuyant sur des travaux de recherche, d'essayer de dresser une typologie des formes administratives ou fonctionnelles que peut prendre ce concept.

Un premier critère important qui permet de différencier les expériences concerne les **fonctionnalités** du guichet : le guichet peut être, soit un service purement **informationnel** mettant à la disposition des administrés des informations administratives dont il a besoin pour mener à bien une démarche ; soit un service **transactionnel** offrant aux administrés des facilités pour réaliser ces démarches administratives en ligne.

[5] Bent S., Kernaghan K., Marson Br, 1999, p.2

Cette idée est d'ailleurs reprise dans la rapport belge réalisé dans le cadre du réseau COST A14[6] :

Guichet unique		
Informationnel	Bureau d'information	Information générale non interactive sur l'organisation
	Téléinformation	Information générale sur l'organisation avec possibilité d'être en ligne avec le service adéquat
	Téléchargement	Téléchargement de formulaires et documents électroniques
Transactionnel	Télédéclaration	Remplissage de formulaires électroniques
	Téléprocédure	Gestion électronique d'une procédure administrative basée sur de multiples contacts entre les départements de l'administration et le citoyen
	Télépaiement	Paiement électronique d'un document, d'un service ou d'une procédure rendue par l'administration

Figure 1. OSG - TELEGUICHET

Le deuxième critère est plus **organisationnel,** il concerne le caractère **intégré ou non du service** offert par le guichet unique. Par guichet intégré , nous entendons l'offre d'un service organisé autour du parcours administratif réel et complet que doit accomplir le citoyen pour réaliser une démarche administrative, et ce même si ce parcours passe par plusieurs administrations ou services administratifs. Ce caractère intégré suppose souvent des ré-organisations importantes tant au niveau du back-office administratif qui supporte ce parcours dans le sens d'une coopération renforcée entre services, qu'au niveau du parcours lui même, dans le sens d'une simplification des procédures et des documents qui les sous-tendent. A l'inverse, dans le cas d'un service non intégré, le guichet unique « se contente » de mettre à disposition de l'administré différents formulaires ou documents, à charge pour lui de recomposer le parcours administratif complet.

1.2.3 La typologie

Ces deux critères suffisent à eux seuls à réaliser une typologie, telle que présentée par le Dr Claire Lobet-Maris[7]. Voici cette typologie :

Guichet unique	*Informationnel*	*Transactionnel*
Non intégré	First stop of information	Convenience Store
Intégré	-	True One Stop

Figure 2. OSG - TYPOLOGIE

[6] Lobet-Maris C., van Bastelear B., 1999, p.4
[7] Lobet-Maris C., 2001, p.2

Cette typologie donne une première idée des guichets uniques dont il existerait trois formes majeures, ce qui a d'ailleurs été constaté dans l'étude européenne sur le réseau COST A14[8].

Le « ***first stop of information*** » représente un bureau d'information. Il vise essentiellement à l'information du public au travers d'un seul point d'accès, physique ou virtuel. Il propose une information simple relative aux services offerts par une ou plusieurs administrations. Par information, on entend ici lieux et heures d'ouvertures, personnes de contact et procédures à suivre. Le service reste quant à lui inchangé.

Le « ***multiple service shop*** » ou « ***convenience store*** » permet d'accomplir différents types de procédures administratives, toujours à partir d'un seul point d'accès, physique ou virtuel. La procédure, ou le service interne, est peu voire non modifié, même si le citoyen en voit sa forme améliorée.

Le « ***one stop shopping*** » ou « ***true one stop*** » développe une approche complète de la procédure administrative, même si cette dernière concerne divers niveaux de pouvoir. On parle alors de service intégré centré sur la demande du citoyen.

Ce dernier type de guichet unique suppose une réorganisation complète de la forme mais aussi du fond, c'est-à-dire des procédures administratives et des systèmes sous-jacents. Le Dr Claire Lobet-Maris va d'ailleurs dans ce sens : *« A une administration organisée verticalement autour de compétences départementales, le guichet unique suggère une structuration plus horizontale des compétences, autour d'une approche intégrée de la demande de l'usager »*[9] .

La réalité, telle qu'on peut la constater dans les rapports nationaux, amène à reconsidérer le positionnement du guichet unique de type « ***first stop of information*** ». Ce guichet unique représente le plus souvent un bureau d'information départemental, mais on rencontre également d'autres systèmes tels que des bureaux d'information nationaux ou encore thématiques. Ces derniers ont la particularité de nécessiter une coopération organisationnelle forte afin de présenter une information cohérente et complète au citoyen .Cette réflexion conduit à la définition d'un quatrième type de guichet unique, à savoir le guichet unique « ***Integrated Portal of Information*** ».

Le « ***Integrated Portal of Information*** » représente un bureau d'information qui vise à l'information du public au travers d'un seul point d'accès, physique ou virtuel. L'information présentée est avant tout centrée sur la procédure administrative et la demande du citoyen.

La typologie peut être revue de la manière suivante :

Guichet unique	*Informationnel*	*Transactionnel*
Non intégré	First stop of information	Convenience Store
Intégré	Integrated Portal of Information	True One Stop

Figure 3. OSG - TYPOLOGIE AVANCEE

[8] Hagen M, Kubicek H., 1999, p.8
[9] Lobet-Maris C., 2001, p.8

1.2.4 Facteurs d'influences

La mise en place de ces types de guichets uniques est influencée par différents facteurs. Selon Hagen et Kubicek, les facteurs suivants influencent ce concept[10] :

- ***le cadre légal*** : les réformes et les lois déterminent le cadre légal de l'OSG dans chaque pays, en particulier en ce qui concerne l'authentification et la signature électronique de l'administré ainsi que la protection des données.

- ***la technologie*** : il existe une grande disparité technologique entre les différents Etats, voire même entre les niveaux de pouvoir d'un même Etat. Des problèmes d'infrastructure existent, comme le degré d'informatisation ou la sécurité des données, et s'ajoutent aux problèmes de standardisation.

- ***l'organisation*** : un modèle organisationnel approprié doit existé afin de soutenir ces réformes. La mise en place d'un tel concept est confrontée aux besoins des parties en présence, c'est-à-dire peuvent-elles en retirer des bénéfices ? Les problèmes de coopération entre les différentes entités doivent donc être résolus ou aplanis.

- ***l'économie*** : de telles réformes demandent aussi des moyens financiers importants, moyens octroyés par un financement interne ou via un fond européen. La coopération du domaine privé est parfois requise afin de mener à bien certains projets.

[10] Hagen M, Kubicek H., 1999, p.21-24

1.3 Les approches nationales du guichet unique

La présentation des approches nationales permet d'illustrer les différents types de guichets uniques. Les exemples ont été choisi avec soin afin de présenter un ensemble de réalisations que tout un chacun a la possibilité de rencontrer dans la vie courante et sous des formes diverses.

1.3.1 Cadre de l'enquête européenne

L'étude européenne[11] sur le réseau COST A14 s'est effectué en 1999 et concernait 11 pays de l'Union Européenne (l'Allemagne, l'Autriche, la Belgique, le Danemark, l'Espagne, la Finlande, la France, l'Irlande, l'Italie, la Grande-Bretagne et les Pays-Bas).

Chaque pays participant à l'étude a fourni un rapport contenant une sélection de 10 cas basés sur les critères méthodologiques suivants :

- le projet doit avoir dépassé la phase purement conceptuelle
- le projet doit être basé sur l'usage de nouvelles technologies et inclure une intégration organisationnelle ou une réforme administrative similaire
- le projet doit permettre des transactions avec les administrés
- le projet doit concerner au moins deux départements administratifs différents

Il leur a aussi été demandé de relever les barrières et les facteurs de succès rencontrés lors de la mise en place du guichet unique. Les points suivants ont été pris en compte pour effectuer ce relevé :

- coopération organisationnelle
- intégration des processus existants
- infrastructure technologique
- aspect légal
- coûts
- bénéfices réciproques
- interactions avec d'autres initiatives

1.3.2 Quelques constatations

Les rapports montrent que plusieurs supports technologiques ont été utilisés afin de mettre en place les guichets uniques. Les quatre canaux suivants ont été utilisés :

- comptoir ou guichet d'accueil
- site Web
- bornes interactives
- call-center

[11] Hagen M, Kubicek H., 1999

Même si certains guichets uniques sont réalisés au travers d'un regroupement physique des services, les nouvelles technologies sont aussi utilisées. Les outils présentés ci-dessous font souvent partie intégrante d'une solution de guichet unique utilisant les nouvelles technologies :

- les systèmes de workflow permettent la gestion d'un ou plusieurs flux administratifs, intra ou interorganisationnel.
- les certificats électroniques permettent l'authentification et la signature électronique
- les formulaires électroniques permettent de fournir les différents documents adéquats, à remplir en ligne ou bien à imprimer pour être expédier par des moyens plus classiques
- l'intégration aux systèmes d'information existants

Il est intéressant de noter que la majorité des développements de guichet unique répertoriés dans les rapports nationaux sont basés sur des comptoirs ou guichets d'accueil en privilégiant le changement organisationnel plutôt qu'une modification des systèmes d'informations supportant la procédure administrative.

Les expériences relatées dans ces rapports confirment que le guichet unique le plus avancé, c'est-à-dire le « True One Stop » , est celui qui est le plus difficile à mettre en place tant les problèmes administratifs et organisationnels sont complexes. Il faut peut-être mettre cela en relation avec la difficulté d'identifier les besoins des citoyens en matière de procédures intégrées.

Il est peut-être plus étonnant que les administrations locales soient celles qui ont le plus mis en place de guichets uniques. Cela est peut-être dû à la complexité institutionnelle des états, même si les stratégies de ces derniers en ce domaine sont assez contrastées. En effet, certains états n'ont pas de stratégie, favorisant les expériences ou projets pilotes, tandis que d'autres construisent un système cohérent et unifié pour l'administration ou encore sont pris par la création d'un cadre légal adapté et complet à l'usage des guichets uniques dans les administrations.

1.3.3 First Stop of Information

Vehicle Registration Tax Information Kiosk, Irlande[12]

En Irlande, la taxe d'enregistrement des véhicules est assez difficile à calculer. Elle fait intervenir une série de paramètres, tels que le modèle du véhicule, son type ou le carburant utilisé. De plus, cette taxe est basée sur le prix courant du marché, ce qui fait qu'elle est ajustée selon les fluctuations de celui-ci. Le calcul de cette taxe étant des plus complexe, l'administration est assaillie par les demandes émanant de particuliers ou de sociétés.

La *Revenue Commissioners*, en collaboration avec le département de l'environnement, a mis en place un système de borne interactive permettant à tout citoyen de connaître le montant de la taxe selon les paramètres introduits. Ce système est alimenté

[12] Bates A J., 1999

par une base d'informations reprenant les données de plus de 10 000 véhicules. L'administration se sert aussi de cette base d'informations afin de continuer à servir le citoyen qui en fait la demande.

Téléphone Vert, Belgique[13]

Le projet Téléphone Vert de la Région Wallonne est un centre d'appel dont l'accès est gratuit pour l'ensemble des citoyens. Il s'agit d'un point unique où chaque citoyen peut obtenir des informations sur l'ensemble des compétences détenues par la Région Wallonne. Ce service couvre entre autres :

- l'habitat : aide régionale à la construction et à la réhabilitation de bâtiments, ...
- l'information économique : aide et fonds à l'investissement et l'innovation, aide à l'emploi, ...
- l'énergie : aide et fonds à l'économie d'énergie, ...
- dettes et emprunts : aide et conseils pour les citoyens ayant des problèmes financiers importants

Le service permet d'aider le citoyen ou le dirige vers le service régional approprié. Il permet une diminution des coûts en désengorgeant les administrations.

Afin de rendre ce service efficace, chaque fonctionnaire du centre est spécialisé dans un domaine. De plus, une structure complémentaire composée d'autres fonctionnaires permet de résoudre les cas les plus complexes. Une base de données reprend l'ensemble des informations.

Le centre d'appel, opérationnel depuis 1989, a été renforcé par 12 bureaux d'information répartis sur le territoire de la région. Un site web doit compléter ce guichet unique.

1.3.4 Convenience Store

"Diba", The Province of Barcelona Telematics Network, Espagne[14]

La province de Barcelone a développé un réseau permettant de fournir de l'information aux administrations locales et de faciliter les démarches administratives pour le citoyen et l'administration.

Au travers d'Internet, il est possible de demander, de télécharger ou de remplir divers formulaires liés aux finances et aux activités économiques, à la population ou encore au service social.

A l'origine, ce réseau a été crée comme un outil d'administration servant à améliorer la communication entre les administrations locales et l'administration provinciale. Au travers ce rapprochement entre administrations, la province de Barcelone a amélioré la rapidité et la qualité de son service, tout en établissant une collaboration

[13] Lobet-Maris C., van Bastelear B., 1999, p.21
[14] Gallego R., Rosetti N., Ysa T., 1999, p.4 et p.12-14

horizontale entre administration. Finalement, ce réseau a été étendu aux citoyens, aux sociétés et à d'autres organismes.

I-Forms, Angleterre[15]

Le projet I-Forms (Intelligent Form) est un projet pilote du gouvernement mettant en évidence qu'un portail est capable de traiter des données venant des citoyens et de les distribuer aux différentes administrations concernées. Ce guichet unique reprend les informations venant de 4 formulaires émis par 3 départements. Le citoyen doit valider le formulaire électronique avant que ce dernier ne soit distribué aux administrations concernées. La validation est effectuée en signant électroniquement le formulaire.

Ce projet a démontré que les formulaires électroniques peuvent être utilisés afin d'améliorer le service offert au citoyen sans modifier les procédures et les systèmes d'informations des administrations.

1.3.5 True One Stop

PBFlow, Belgique[16]

Le projet PBFlow a été développé en 1996 par l'université de Namur, la Région Wallonne et les autorités communales de la ville de Namur. Il fait partie d'un programme nommé ***Péricles***, **P**rogram for **E**xtending **R**esources in **I**nformation and **C**ommunication by a **L**ocal **E**xchange **S**ystem. Ce programme, coordonné par le professeur François Bodart des Facultés Université Notre-Dame de la Paix de Namur (FUNDP), a pour but de promouvoir l'utilisation des technologies de l'information et des communications.

Le projet PBFLow a été crée afin d'améliorer la procédure de délivrance des permis de bâtir. Cette procédure, longue et obscure, implique en plus du demandeur et de l'architecte, différents niveaux de pouvoir, dont l'administration locale et l'autorité régionale. PBFlow a donc été conçu pour être un outil générique de traitement des procédures interorganisationnelles.

PBFlow s'intègre avec les différents systèmes d'information des acteurs, ce qui inclus l'échange d'e-mail, la soumission et la signature de documents électroniques. Il permet aussi d'obtenir des informations sur l'état de la procédure et des acteurs mis à contribution. Finalement, il est un outil de classification et d'archivage.

Le projet ayant réussi tous les tests, un partenariat avec le secteur privé a été conclu. Il aboutit à la création d'une plate-forme administrative appelée AdmiPro.

[15] Bellamy C., Brewer N., Petrie A., 1999, p.10
[16] Lobet-Maris C., van Bastelear B., 1999, p.19

Donegal County Council, Irelande[17]

L'administration de Donegal a décidé d'avoir une approche plus intégrée de la délivrance de services aux citoyens. Il a été décidé de décentraliser les services de l'administration et de créer un bureau par secteur électoral, qui sont au nombre de six.

Chaque bureau reprend l'ensemble des services fournis par l'administration centrale et a la possibilité d'accueillir d'autres organisations fournissant un service social et un service d'information au public. L'administration se rapproche ainsi du citoyen, tout en améliorant la qualité de son service.

Integrated window for business activities, Italie[18]

Jusqu'en 1998, toute autorisation liée à une activité économique implique, outre l'administration centrale, toute une série d'administrations locales. La procédure est donc longue et contraignante. Depuis 1998, la responsabilité de toute action administrative relative à l'activité économique de sociétés privées et publiques est du ressort des communes, même si ces dernières ne délivrent pas l'ensemble des autorisations.

Chaque administration locale doit mettre en place un système permettant de réaliser ces opérations administratives à partir d'un seul point d'accès et d'obtenir toutes autorisations requises pour exercer une activité économique.

Par exemple, la ville de Bologne a mis en place le guichet unique sous la forme d'un bureau central. Bien qu'une partie de la procédure soit toujours sous format papier, un système d'information est mis en place petit à petit. Il doit permettre :

- de demander et de remplir tout formulaire nécessaire à la démarche administrative,
- de prendre connaissance des informations du dossier et de connaître l'état d'avancement de la procédure,
- d'obtenir les autorisations dès qu'elles sont produites par les différentes administrations et collectées par le guichet unique,
- de demander la tenue de réunion avec les administrations si cela est nécessaire lors de la démarche administrative.

[17] Bates A J., 1999, p.30
[18] Marsocci P., Salza S., 1999

Chapitre 2 Illustration d'une typologie : Application à PBFlow

Ce chapitre introduit le projet AdmiPRO - PBFlow. Les aspects fonctionnels et techniques du projet sont présentés au lecteur. Ce chapitre se termine par le classement du logiciel AdmiPRO dans la typologie présentée précédemment.

2.1 Contexte

La Région Wallonne, la ville de Namur et les Facultés Universitaires Notre-Dame de la Paix (FUNDP) ont financé et participé au projet de développement d'un système original de gestion électronique de dossiers administratifs appelé « PBFlow ». Ce projet a débuté le premier janvier 1997 et s'est terminé le 30 avril 1999.

La propriété de « PBFlow » a été transférée à WIN s.a. qui a confié à NSI s.a. un ensemble de prestations visant à faire évoluer le logiciel « PBFlow » vers une nouvelle plate-forme baptisée « AdmiPRO ». Cette évolution se fait en 2 phases :

- la première phase comprend le développement de la composante générique mono-serveur et le développement de l'environnement graphique de paramétrage du système
- la seconde phase comprend le développement des fonctions d'archivage, la prise en charge de l'environnement multi-sites, multi-serveurs et la mise en place des modules de sécurité d'exploitation de type sauvegarde

La suite de ce chapitre ne concerne que la phase I, en cours actuellement.

2.2 Objectifs du projet AdmiPRO

Sur base de l'expérience du projet PBFLow, WIN s.a. et NSI s.a. veulent créer une plate-forme administrative offrant des fonctionnalités originales de gestion souple du flux de travail et de gestion intelligente des dossiers électroniques. Le projet n'est pas limité à la problématique de la délivrance du permis de bâtir et doit pouvoir traiter tout type de procédure.

Afin de répondre au nouveau cahier des charges, les objectifs suivants[19] sont définis :

- **Intégration des documents et des processus**

  AdmiPRO doit intégrer la ***gestion de documents électroniques*** (archivage, digitalisation, gestion de versions, aide à l'édition, etc.) à la ***gestion des processus*** (routage des tâches, des documents, suivi d'avancement, reporting, etc.). L'utilisateur du système doit pouvoir accéder de manière transparente à la fois aux fonctions de ***gestion de dossiers électroniques*** (liste des dossiers présents dans son service, visualisation du contenu des dossiers, date d'introduction dans l'organisation, etc.) et aux ***fonctions d'organisation de son travail*** (liste de nouvelles tâches, liste des tâches urgentes, liste des tâches en retard, etc.)

- **Gestion des dossiers inter-organisationnels**

  AdmiPRO doit assurer la ***gestion des dossiers inter-organisationnels***. Les différentes organisations et le processus de traitement des dossiers administratifs doivent être modélisés.

- **Amélioration des pratiques administratives**

  AdmiPRO doit améliorer la *transparence* des traitements de dossiers administratifs en donnant, à tout moment, l'état d'avancement d'un dossier et en permettant de visualiser la contribution de chacun des agents. ***AdmiPRO doit remplir les fonctions "téléprocédures" et "suivi" des guichets uniques.***

- **Intégration des systèmes d'informations existants**

  AdmiPRO doit être capable d'échanger des informations avec les systèmes d'informations existants.

- **Disponibilité du système**

  L'architecture AdmiPRO doit assurer le déploiement de l'application distribuée au sein du WIN s.a. tout en rencontrant les exigences en matière de sécurité, performances, et robustesse.

- **Application au secteur privé**

  AdmiPRO doit pouvoir s'intégrer dans toutes les entreprises ayant à traiter des dossiers faisant intervenir des acteurs externes à l'organisation (dossiers de contentieux, suivi de contrats, ...).

[19] NSI s.a., "AdmiPRO - Fiche Produit", 2001

Le projet se définit comme suit : ***"AdmiPRO assure la gestion et la circulation des dossiers électroniques entre organisations (aspects inter-organisationnels) et entre directions et services d'une organisation (aspects intra-organisationnels). Il agit en tant qu'outil fédérateur et garantit la standardisation des échanges entre les différents acteurs."***

La figure ci-dessous représente cette définition.

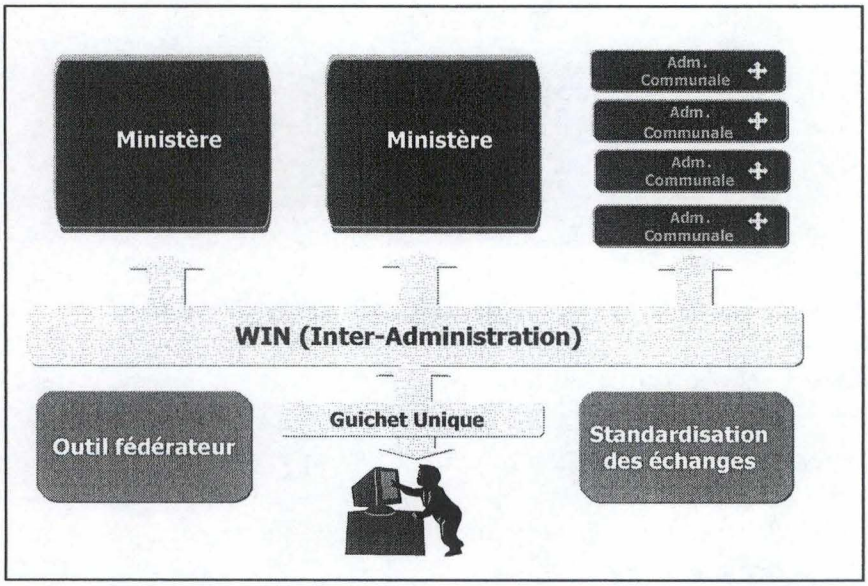

Figure 4. ADMIPRO - CONCEPT D'ADMIPRO

La complexité de telles solutions conduit vers une solution générique ; base solide pour assurer la généralisation du système à un cadre inter-organisationnel.

2.3 Description fonctionnelle du logiciel AdmiPro

Sur base des objectifs fixés, les fonctionnalités d'AdmiPRO couvrent les domaines suivants[20] :

- gestion de l'organisation
- gestion des données structurées
- gestion des documents
- définition des processus
- exécution des processus intra-organisation
- suivi des processus intra-organisation
- exécution des processus inter-organisation
- suivi des processus inter-organisation

Ces fonctionnalités sont détaillées dans les points ci-dessous.

2.3.1 Gestion de l'organisation

La gestion de l'organisation reprend :

- description de la structure organisationnelle, tels que les services et les départements
- description des compétences organisationnelles, tels que les projets et les missions
- description des personnes et des rôles joués par ces dernières
- affectation des personnes au sein de la structure organisationnelle
- gestion de la disponibilité des personnes
- consultation de l'annuaire organisationnel

2.3.2 Gestion des données structurées

La gestion des données structurées comprend :

- partage de l'information
- fonction de backup des données
- fonctions de transformation regroupées en boîtes à outils administratives
- contrôle d'accès
- indexation et recherche par mots-clés
- génération de documents à partir des informations structurées

[20] NSI s.a., "AdmiPRO - Fiche Produit", 2001

2.3.3 Gestion des documents

La gestion des documents reprend :

- recherche "full text"
- gestion de modèles de documents
- indexation et recherche des documents
- archivage des documents
- gestion des versions
- gestion des signatures électroniques
- confidentialité et sécurité des documents stockés et échangés
- consultation partagée des documents
- mécanisme de signatures électroniques des documents

2.3.4 Définition des processus

La définition des processus comprend :

- ordonnancement des traitements par manipulation de logigrammes
- prévision des délais (agenda jours ouvrables fériés, ..)
- données variables des traitements
- résultats des traitements
- attribution de la réalisation des traitements aux rôles organisationnels et/ou aux organisations
- outil de validation
- consultation de la description des traitements par les intervenants (formation, référentiel, ...)

2.3.5 Exécution des processus intra-organisation

L'exécution des processus intra-organisation reprend :

- distribution des dossiers et des traitements au sein de l'organisation
- gestion de la charge individuelle de travail (en cours, urgent, en retard)
- réalisation des tâches
- initialisation et gestion de traitements ad hoc (demande d'information, délégation de production de documents, envoi pour avis)
- initialisation de traitements prédéfinis
- gestion des droits
- gestion des délais
- proposition du travail à effectuer via les boîtes de travail des utilisateurs

2.3.6 Suivi des processus intra-organisation

Le suivi des processus intra-organisation comprend :

- visualisation graphique de l'état d'avancement des dossiers
- notification des dépassements de délai
- langage d'interrogation de l'historique des traitements
- génération de rapports d'activités par intervenant, par service, par zone géographique
- notification par e-mail
- consultation et visualisation des tâches intra-organisationnelles

2.3.7 Exécution des processus inter-organisation *(Phase II)*

L'exécution des processus inter-organisation reprend :

- distribution des dossiers et des traitements entre organisations (alimentation des boîtes de travail des organisations)
- gestion des demandes d'informations ad hoc entre organisations
- initialisation de traitements
- initialisation des recours éventuels

2.3.8 Suivi des processus inter-organisation *(Phase II)*

Le suivi des processus inter-organisation comprend :

- situation des dossiers par organisation
- notification des dépassements de délai et activation des recours
- certificateur des échanges de documents entre organisations (accusé de réception, date d'envoi, date de réception, ...)
- génération de rapports d'activités par organisation
- visualisation graphique du flux entre organisations
- notification par e-mail

2.4 Architecture fonctionnelle

L'architecture fonctionnelle[21] de l'application AdmiPRO est présentée ci-dessous. Cette architecture se compose d'un environnement de paramétrage et d'un environnement d'exécution. L'environnement de paramétrage offre les outils permettant de définir les procédures et la manière de traiter les dossiers administratifs tandis que l'environnement d'exécution exploite cette définition pour permettre aux agents d'organiser et de réaliser leur travail quotidien.

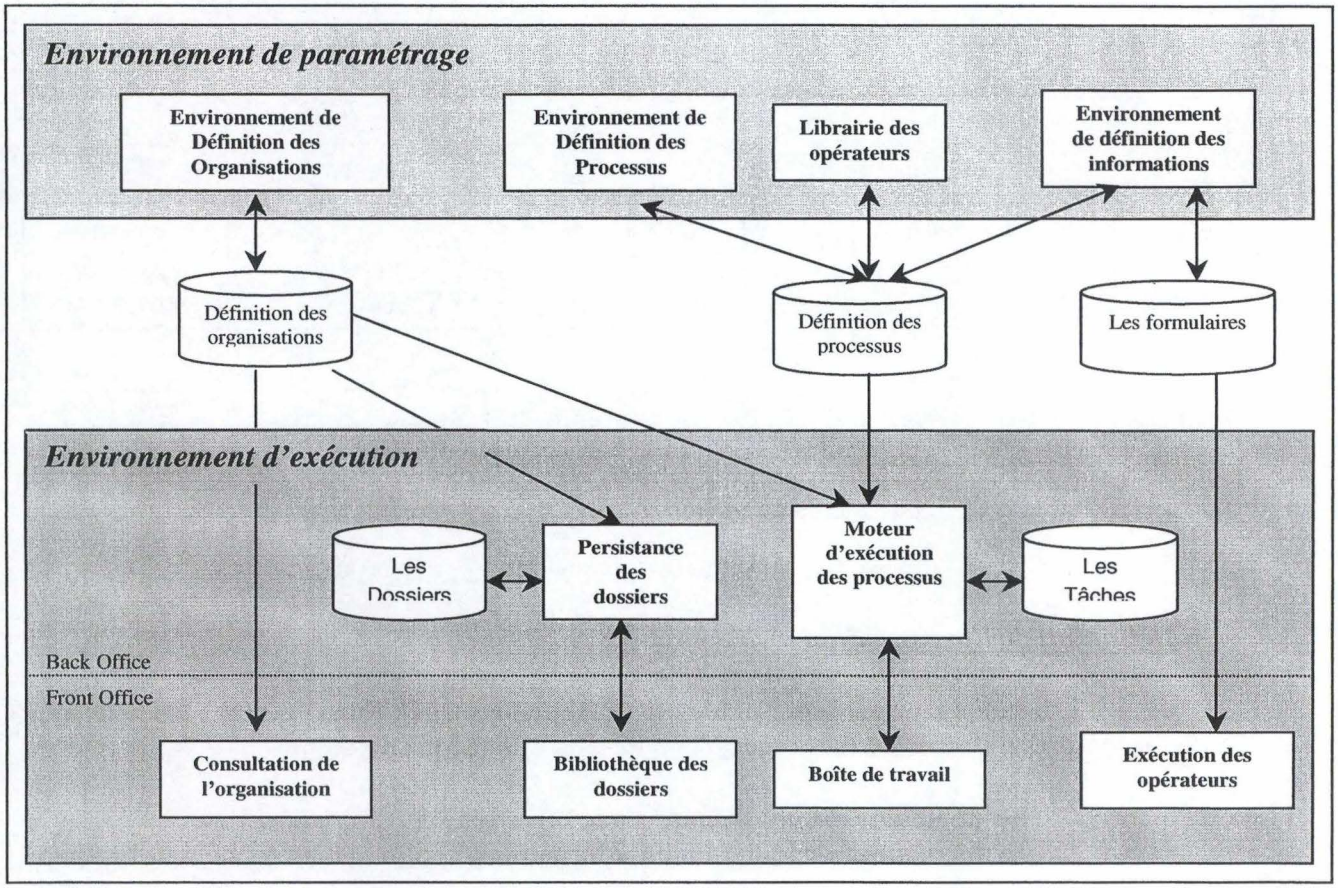

Figure 5. ADMIPRO - ARCHITECTURE FONCTIONNELLE

L'environnement de paramétrage offre des fonctions de définition des organisations, de définition des informations, de définition des processus et de définition de l'utilisation des opérateurs.

L'environnement d'exécution comprend des fonctions « BackOffice » et des fonctions « FrontOffice ». Les fonctions « BackOffice » sont le moteur d'exécution des procédures et la persistance des dossiers. Les fonctions « FrontOffice » sont les fonctions directement accessibles par l'utilisateur : la boîte de travail des utilisateurs, la bibliothèque des dossiers, la consultation de l'organisation et l'exécution d'opérateurs.

[21] Poos W., 1999.

2.4.1 Environnement de paramétrage

Selon la documentation de NSI s.a., l'environnement de paramétrage permet de définir les « bonnes manières » de traiter les dossiers administratifs. Ses différentes composantes permettent de définir le QUI, le QUOI et le COMMENT.

La définition du ***QUI*** est assurée par les fonctions de ***définition de l'organisation***, la définition du ***QUOI*** est assurée par les fonctions de ***définition des informations*** et la définition du ***COMMENT*** est assurée par les fonctions de ***définition des processus*** complétées par la librairie d'opérateurs.

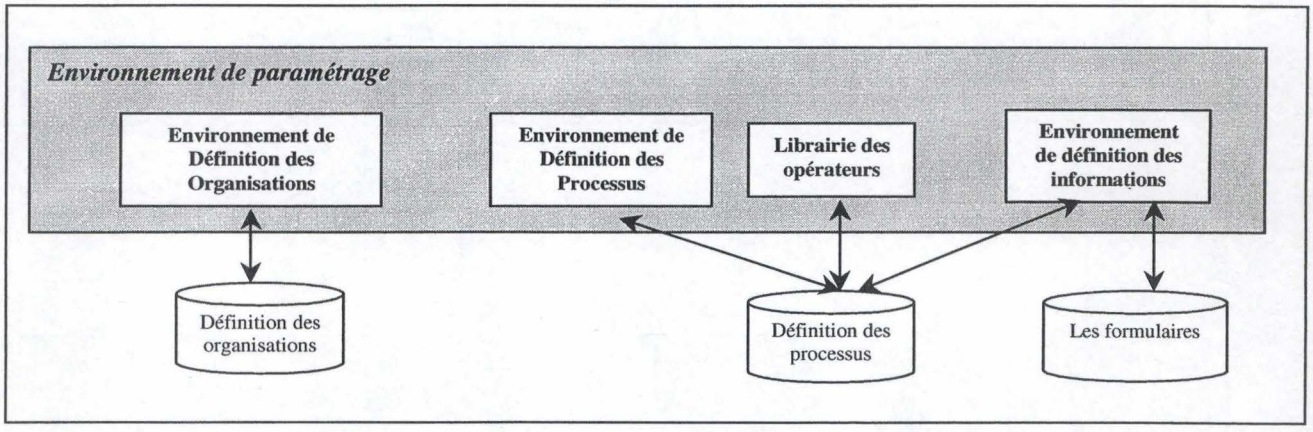

Figure 6. ADMIPRO - ENVIRONNEMENT DE PARAMETRAGE

Définition de l'organisation

L'organisation est représentée par trois grandes catégories d'objets : les **acteurs**, les **groupes** et les **rôles**. Ces objets sont décrits de la façon suivante :

- un **acteur** est un membre d'une organisation
- un **groupe** est un ensemble d'acteurs artificiellement réunis pour produire ou prester un service de manière efficace dans un environnement donné. Généralement, il s'agit des départements et des services des organisations. Les groupes forment un arbre doté d'une relation de composition
- un **rôle** décrit un domaine de compétence. Un rôle peut être « absolu » ou « relatif ». Citons comme exemple de rôle absolu : secrétaire, président, directeur, ... Un rôle relatif est une fonction remplie, non pas de manière globale au sein de l'organisation, mais par rapport à un dossier. Citons comme exemple de rôle relatif : le responsable d'un dossier et l'initiateur d'un dossier
- un **acteur** appartient généralement à un groupe, plus rarement à plusieurs. Il remplit un ou plusieurs rôles dans son organisation.

L'organisation peut donc être décrite comme étant une structure hiérarchique dont les nœuds sont en fait des groupes ou des rôles et dont les feuilles représentent les membres de cette même organisation.

Définition des informations

Du point de vue des informations, le dossier est l'élément central. Il joue plusieurs rôles qui sont :

- représenter l'entité qui regroupe toutes les informations qui concernent une même "transaction" au sein du flux de travail.
- être la source principale des informations dont disposera chaque acteur pour réaliser les tâches qu'il assume.
- être le vecteur (le support) principal qui assure la communication des informations entre les tâches successives.
- refléter l'état d'avancement des tâches et de constituer par les documents qu'il contient la trace complète et inaltérable du cheminement des informations.

Une **catégorie de dossiers** est formée d'un ou de plusieurs types de documents prédéfinis. Une instance d'une catégorie de dossiers est un dossier. Outre des paramètres d'identification, la catégorie de dossier comprend :

- des types de documents non-structurés
- des types de documents structurés
- une procédure de traitement à appliquer

Les **paramètres d'identification** sont des informations structurées: un objet, un demandeur, un bien, une adresse, … Généralement, ces informations sont connues du système d'information de l'organisation. On y retrouve des bases de données « Personnes physiques », « Personnes Morales », « Communes », etc.

Un **type de document** représente une catégorie de document qui a une existence réelle dans l'organisation et dont la description peut être effectuée avant l'exécution du flux. Souvent, un type de document correspond à un modèle de document administratif qui a une existence légale (ou du moins réglementaire) dans les organisations. Un type de document peut être structuré ou non-structuré.

Un type de document **structuré** est un type de document dont le contenu peut être représenté par un formulaire. Le formulaire permet de manipuler des valeurs "spécifiques" et "numérisables" associées à un document. Un type de document **non structuré** est un type de document dont la représentation peut être informatisée mais dont le contenu ne peut être structuré en couple champ/valeur. Un exemple de ce type de document est une photo.

La fonction d'avertissement permet de définir un ensemble de rôles qui seront avertis lorsqu'une instance de ce type de document sera publiée dans le dossier.

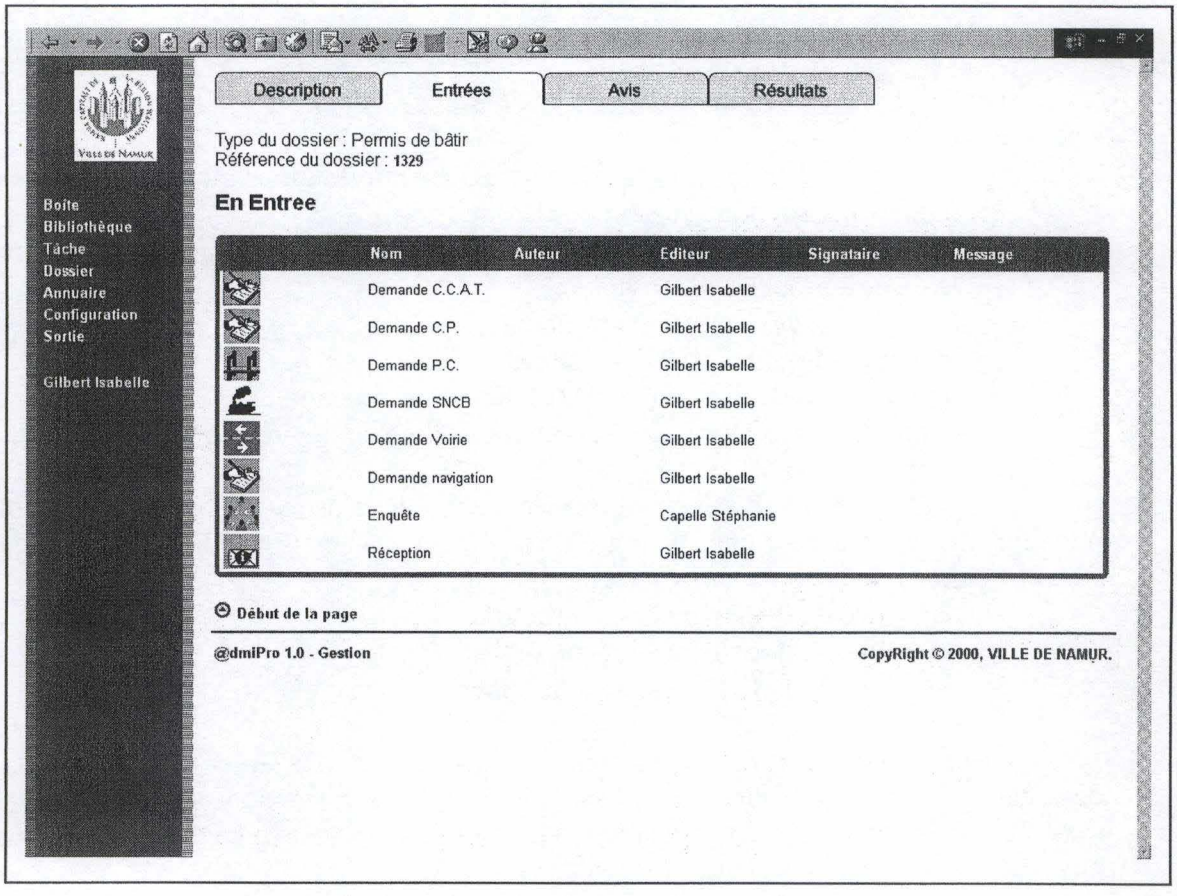

Figure 7. ADMIPRO - DOCUMENTS EN ENTREE D'UNE TACHE D'UN DOSSIER PBFLOW 108

Définition des processus

Une procédure est la description de la « bonne manière » de traiter un dossier, elle spécifie :

- la définition des **types de tâches à réaliser** pour assurer l'évolution de ce dossier jusqu'à sa clôture
- la description de **l'enchaînement** de ces types de tâches
- la spécification des **types de données nécessaires** à leur exécution,
- la spécification des **types de résultats attendus**,
- la manière dont **différents acteurs peuvent participer à leur réalisation** ainsi que de la spécification de leur **délai de réalisation.**

Un **type de tâche** est une étape de la procédure. Un type de tâche correspond à un traitement dont l'exécution sera assumée par un acteur. Le traitement est défini par un ensemble d'actions proposées. Une **action** est l'application d'un opérateur à un document ou à un dossier. La définition des compétences nécessaires pour réaliser une tâche est la **règle d'assignation** du type de tâches.

Certaines procédures sont liées à un délai. La durée est relative à un type de tâche ou à un circuit de types de tâche. Une durée a un nombre de jours autorisés qui représentent des jours ouvrables ou des jours 'calendrier'. Le nombre de jours autorisés peut être modifié (augmenté, diminué, suspendu) en fonction d'occurrence d'événements

particuliers (ex. démarrage d'une enquête publique, production d'un avis négatif, ...) survenant dans une instance de catégorie de dossier.

Lorsqu'une durée est dépassée on peut, par exemple :

- générer un document par défaut et reprendre le flux.
- initialiser une tâche.
- avertir le responsable de la catégorie de dossier.
- avertir le réalisateur de la tâche.
- terminer les tâches concernées.
- ...

En plus des actions 'prédéfinies' liées au dépassement de délai, AdmiPRO donne aux développeurs de flux la possibilité de programmer ou de lancer une action particulière directement liée au domaine d'application de la catégorie de dossier concernée. Cette capacité illustre l'ouverture et la modularité de l'architecture fonctionnelle.

Librairie d'opérateurs

La librairie des opérateurs est la boîte à outils permettant aux acteurs de traiter les dossiers administratifs. Le développeur de flux les associe avec les étapes du traitement des catégories de dossiers. AdmiPRO comprend les opérateurs génériques suivants :

- Signature d'un document
- Production d'un document structuré ou non-structuré

2.4.2 Environnement d'exécution

L'environnement d'exécution permet d'une part de réaliser, de la « bonne manière », les traitements des dossiers administratifs et d'autre part de relater le travail effectivement réalisé.

Dans la documentation de NSI s.a., les fonctions de l'environnement d'exécution sont représentées dans deux catégories, à savoir les fonctions « BackOffice » qui sont des fonctions non directement visibles pour l'utilisateur et les fonctions « FrontOffice » qui sont des fonctions directement manipulables par les utilisateurs.

Le « **BackOffice** » est formé par les fonctions de moteur d'exécution des procédures et par les fonctions de recherche et de persistance des dossiers et des documents.

Le « **FrontOffice** » est formé par les fonctions de la boîte de travail, par les fonctions de consultation de l'annuaire organisationnel, par les fonctions de la bibliothèque des dossiers et par la mise à disposition pour les utilisateurs d'opérateurs tels que la signature électronique de document. Le « **FrontOffice** » agit en tant que portail.

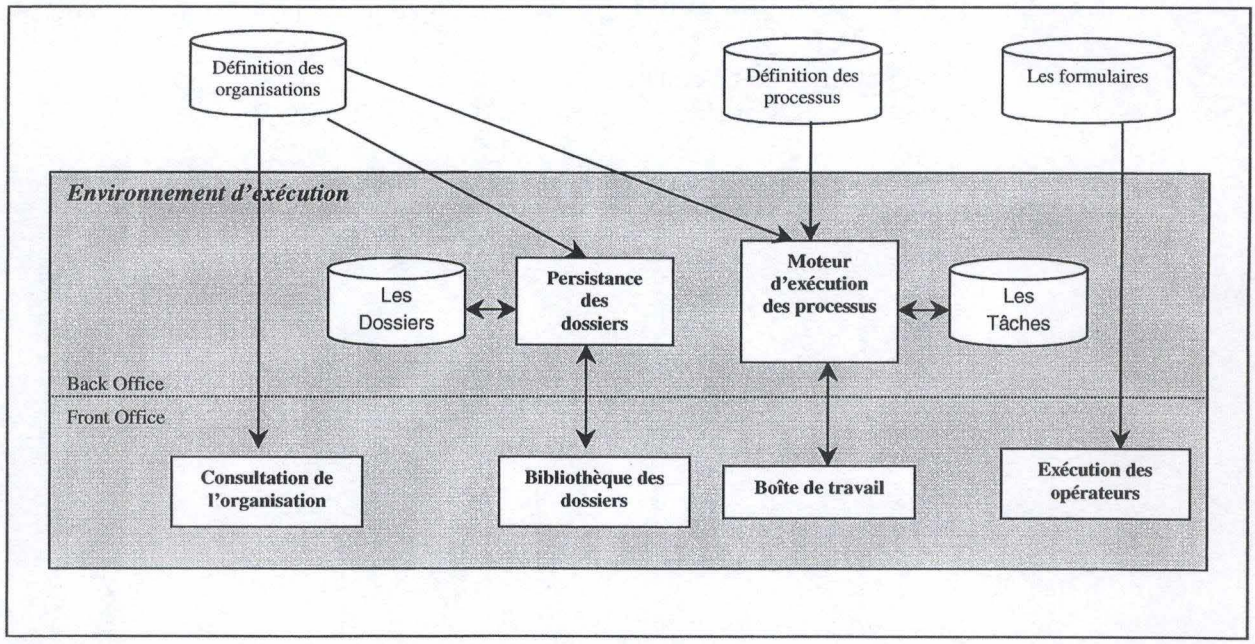

Figure 8. ADMIPRO - ENVIRONNEMENT D'EXECUTION

Le « BackOffice »

Moteur d'exécution des procédures

Le **moteur d'exécution** des procédures est le cœur dynamique d'AdmiPRO, c'est lui qui, en fonction des tâches réalisées par les utilisateurs, synchronise les différentes tâches d'un dossier suivant la description de sa catégorie. Il joue le rôle d'horloge du système puisqu'il avertit les responsables lorsqu'une tâche est non terminée après un certain délai, termine des tâches par défaut, clôture des dossiers suivant la description des contraintes de temps des catégories de dossiers.

Persistance et recherche des dossiers et des documents

La persistance et la recherche comprennent la recherche des dossiers et des documents selon le type, la date ou le responsable du dossier.

Le « FrontOffice »

Boîte de travail

Une **boîte de travail**, telle que représentée ci-dessous, appartient à un utilisateur et lui offre des fonctionnalités qui lui permettent d'organiser et de réaliser son travail quotidien. Elle comprend les objets du modèle des procédures que cet acteur a le droit de manipuler.

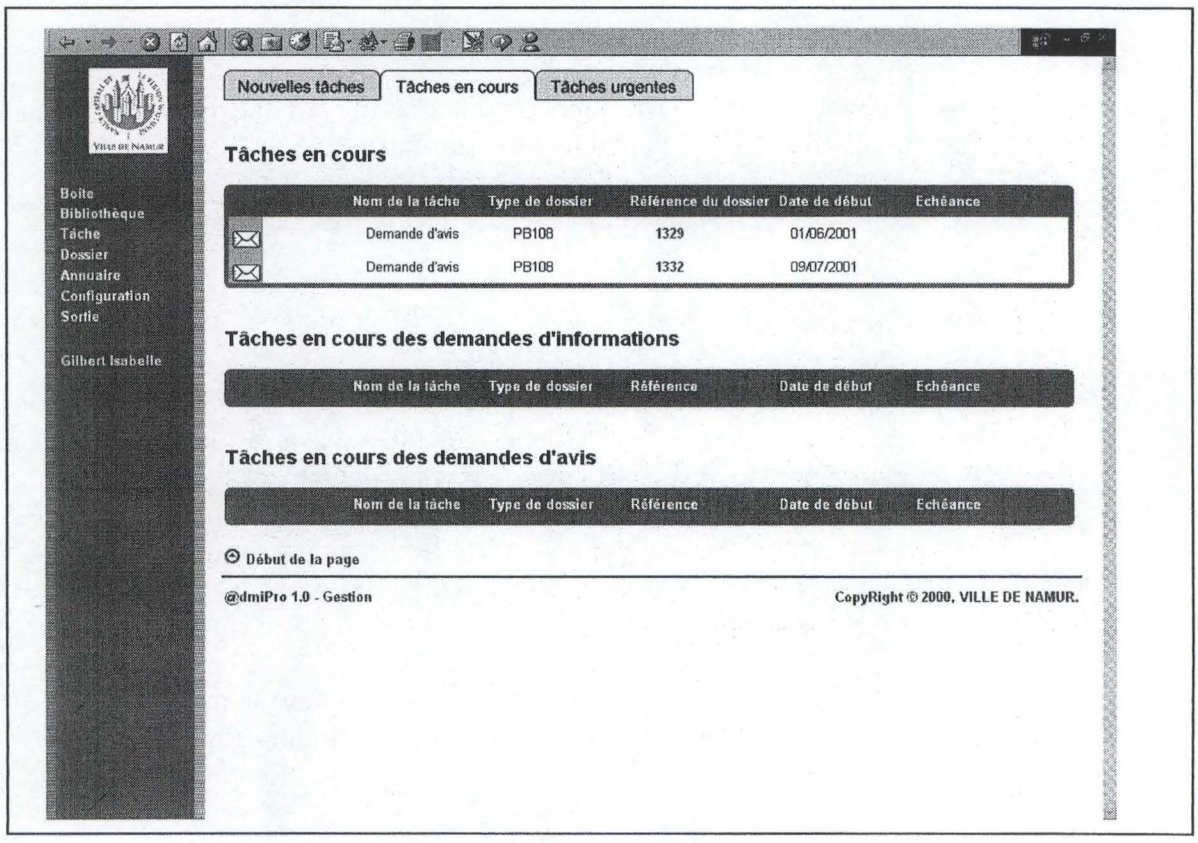

Figure 9. ADMIPRO - BOITE DE TRAVAIL

Bibliothèque de dossiers

La **bibliothèque des dossiers** est la pile de dossiers électroniques auxquels les acteurs d'une organisation ont accès.

Consultation de l'annuaire organisationnel

La consultation de l'annuaire organisationnel comprend la consultation des acteurs, des organisations, des groupes et des rôles. Une recherche par mots-clés peut être effectuée dans l'annuaire électronique.

Exécution des opérateurs

L'acteur se voit proposer, par exemple, la signature électronique d'un document ou encore la génération d'un document par le système.

2.5 Technologies utilisées

AdmiPRO est basé sur la gamme des produits Oracle Corporation. Outre la base de données relationnelles, AdmiPRO intègre le logiciel Oracle Workflow. Ce logiciel assure la définition des processus et l'exécution de ces derniers. Oracle InterMedia est utilisé pour l'intégration des documents dans la base de données. Il permet une indexation et une recherche "full text" de ces mêmes documents. Quant au logiciel en lui-même, il intègre une série de modules basés sur les dernières technologies liées au monde Java.

Aucune installation sur le poste client n'est nécessaire. Un navigateur Web standard suffit amplement afin d'accéder à la plate-forme administrative.

A titre d'information, l'architecture technique est reprise dans les annexes.

2.6 AdmiPRO, guichet unique ?

AdmiPRO est avant tout un système transactionnel dont les différents modules qui le composent sont particulièrement bien adaptés aux téléprocédures. Il peut aussi assurer le rôle de guichet unique de type télédéclaration ou téléchargement.

Au vu de son architecture modulaire, AdmiPRO s'intègre parfaitement dans l'organisation, entre autre grâce à sa représentation organisationnelle et les possibilités d'interfaçage avec les systèmes existants.

AdmiPRO peut donc servir de base à la mise en place des quatres types de guichets uniques (cf. 1.2.3 La typologie) mais il est avant tout un « ***True One Shop*** ».

2.7 Problèmes étudiés

Pour rappel, la mise en place d'un guichet unique est influencée par les facteurs suivants :

- le cadre légal
- la technologie
- l'organisation
- l'économie

Il serait trop long d'aborder l'ensemble de ces facteurs dans le cadre du projet AdmiPRO. C'est pourquoi seulement deux facteurs seront abordés, à savoir :

- l'organisation à travers la mise en place d'un système de représentation organisationnelle.
- le cadre légal à travers la signature électronique et le mécanisme de preuve

Les chapitres suivants décrivent les problèmes posés par ces deux facteurs. Une synthèse des concepts est réalisée et chaque chapitre est clôturé par la présentation d'une solution originale et personnelle.

La représentation organisationnelle devra permettre de modéliser l'organisation dans toute sa complexité, c'est dire modéliser la structure hiérarchique des services et départements, mais aussi la structure hiérarchique entre les membres de l'organisation et les rôles joués par chacun d'entre eux. Les concepts de la solution seront expliqués avant de décrire le processus suivi dans AdmiPRO.

Le cadre légal de la signature électronique et le mécanisme de preuve seront abordés aux travers des lois belges. Les solutions techniques envisagées pour traduire les lois dans la pratique seront justifiées et présentées au travers du logiciel AdmiPRO.

Ces deux facteurs, représentation organisationnelle et cadre légal, peuvent facilement être mis en relation avec la typologie présentée précédemment (cf. 1.2.3 La typologie) :

Guichet unique	*Informationnel*	*Transactionnel*
Non intégré	Représentation organisationnelle	Représentation organisationnelle Signature électronique
Intégré	Représentation organisationnelle	Représentation organisationnelle Signature électronique

Le problème de la représentation organisationnelle se pose quelle que soit le guichet unique. Par contre, le problème de la signature électronique ne se rencontre que dans les systèmes transactionnels.

Chapitre 3 Les annuaires électroniques

Ce chapitre introduit la problématique de la représentation organisationnelle. Les concepts présents dans les services de noms et les services d'annuaires sont expliqués en détails. On évoque alors les différentes possibilités de déploiement et d'intégration dans les organisations avant de décrire le processus suivi dans le projet AdmiPro.

3.1 Problématique de la représentation organisationnelle

Lors de la mise en place de guichet unique, et surtout lorsqu'il s'agit d'un "True Store", l'organisation tout entière y est associée. Mais comment intégrer l'organisation au guichet unique ? Comment représenter sa structure, c'est-à-dire l'ensemble de ces services, de ses membres et du rôle qu'ils y jouent ? Comment s'assurer de la confidentialité et de la distribution des informations représentées ?

Ces problèmes d'intégration, de représentation et de visibilité de la structure organisationnelle sont résolus grâce à l'utilisation des annuaires électroniques. Sans anticiper sur les lignes qui suivent, on peut dire que :

- un annuaire électronique permet de représenter hiérarchiquement des informations
- un annuaire électronique possède des objets et méthodes permettant de modéliser une organisation
- un annuaire électronique offre des outils assurant la distribution et la confidentialité de ses données
- un annuaire électronique garantit le niveau de service

Tous ces points sont développés au travers des lignes qui suivent. Après la synthèse de la terminologie et des concepts des annuaires, on présente les techniques de modélisation des organisations. L'implémentation dans AdmiPRO résultant d'un apport original à la veille technologique est alors justifiée.

3.2Introduction aux annuaires

Application à part entière ou partie intégrante d'un système d'exploitation, les services de noms et d'annuaires permettent de stocker et de gérer un ensemble d'informations.

Les services de noms associent un nom à un objet, et permettent de retrouver sa localisation. Les services d'annuaire vont encore plus loin en associant des attributs à ces noms. Ils intègrent ainsi toutes sortes de ressources disponibles dans une organisation :

- les données des ressources humaines,
- l'équipement et la configuration du réseau,
- l'accès à certaines applications,
- compléments aux systèmes sécurisés

3.2.1 Les bénéfices

Un service de noms ou d'annuaire fournit une vue logique unique des utilisateurs ou des ressources d'une entreprise. Le système, accessible de manière transparente pour tous, est ainsi perçu comme une seule ressource et non plus comme un ensemble de systèmes indépendants les uns des autres. L'avantage de cette vue est de permettre une mise à jour optimale et synchronisée des informations pour l'ensemble des utilisateurs et des applications. Les risques de redondance, la sécurité et les coûts d'administration sont donc mieux contrôlés.

Les services de noms et d'annuaire fournissent donc une solution pour le stockage et la gestion de données en un point unique, permettant ainsi l'intégration des systèmes ou services distribués.

Les services d'annuaires ont un avantage non négligeable sur les services de noms. Ils permettent évidemment de retrouver la localisation d'un objet à partir de son nom mais aussi de stocker des attributs, ou d'un point de vue plus technique, des objets relatifs à ce nom.

3.2.2 Les caractéristiques

Avant toute chose, un service de nom ou d'annuaire est un système coopératif. Il s'agit d'une base de données spécialisées, que l'on appelle aussi « repository ». Son rôle est de faire le lien entre le nom de l'objet et l'objet lui-même, via une convention dans la dénomination du nom.

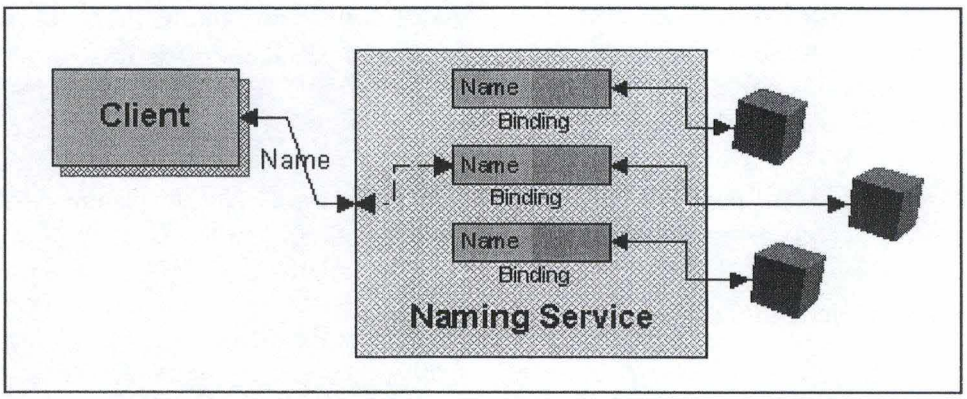

Figure 10. LDAP - SERVICE DE NOM

Néanmoins, un tel service possède des caractéristiques qui le différencient d'une base de données relationnelle classique[22].

La principale caractéristique est qu'il est presque exclusivement accédé en lecture, ce qui fait qu'il est optimisé pour ce type d'accès. Cela implique que les données sont essentiellement statiques.

Etant donné que les mises à jour sont rares, la notion de consistance qui caractérise une base de relationnelle n'est pas une des priorités. La notion de transaction est donc absente.

Vu que ces services n'ont pas besoin d'avoir autant de fonctionnalités qu'une base de données classique, la manière d'accéder à l'information a été grandement simplifiée et optimisée.

[22] Johner H., Brown L., Hinner F.-S., Reis W., Westman J., 1998, p.3

3.2.3 Quelques exemples connus

Voici quelques exemples[23] ...

... de services de noms :

- **DNS (Domain Name System) :** le service des noms de domaines Internet permet la translation entre le nom d'un serveur et son adresse IP. Il est utile de signaler que le DNS est un système d'annuaire distribué, ce qui signifie que le service et les noms sont dispersés sur l'ensemble du réseau Internet.

- **NIS (Network Information System) :** ce service permet aux utilisateurs d'accéder à des fichiers et à des applications sur n'importe quelle machine.

... de services d'annuaires :

- **COS (Common Object Services) Naming :** le service d'annuaire de CORBA permet aux applications de stocker et d'accéder aux références des objets CORBA.

- **LDAP (Lightweight Directory Access Protocol) :** ce service est une version allégée du protocole DAP (Directory Access Protocol) permettant l'accès aux systèmes X.500.

Ce dernier service étant utilisé pour la représentation organisationnelle, il est décrit plus en détail ci-après.

[23] Sundsted T., Janvier 2000

3.3LDAP (Lightweight Directory Access Protocol)

3.3.1 Historique[24]

Le modèle OSI (Open Systems Interconnect) résulte des efforts menés par le CCITT (Consultative Committee on International Telephony and Telegraphy) qui a définit un modèle en sept couches pour le transport de données, allant du transport physique des données aux protocoles applicatifs.

Le service d'annuaire X.500 a été créé en 1988 par le CCITT. Il a évolué depuis pour devenir *ISO 9594, Data Communications Network Directory, Recommandations X.500-X.521.*

Ce standard, toujours connu comme X.500, organise les entrées d'un annuaire de manière hiérarchique afin d'être capable de supporter un nombre important d'informations. Il définit aussi un système de recherche performant afin d'accéder à l'information de manière plus aisée. X.500 définit que le protocole DAP (*Directory Access Protocol*) est utilisé entre un client et un serveur. Ce protocole est basé sur le modèle OSI.

Le désavantage de DAP était d'utiliser l'entièreté du modèle OSI, qui se révèle très lourd à implémenter et à utiliser. LDAP fut alors développé comme une alternative au protocole DAP définissant l'accès au service d'annuaire X500. Il est basé sur le protocole TCP/IP et simplifie les opérations X.500.

Une première version de LDAP est apparue grâce aux travaux de l'Université du Michigan. Ces travaux étaient basés sur les standards *RFC 1487 X.500 Lightweight Access Protocol* et *RFC 1777 Lightweight Directory Access Protocol* tous deux émis par l'IETF (*Internet Engineering Task Force*). La version actuelle de LDAP est la version 3, basée sur le *RFC 2251, Lightweight Directory Access Protocol (v3).*

3.3.2 Protocole ou service d'annuaire

LDAP est un protocole simplifié ayant les caractéristiques suivantes :

- il utilise le protocole TCP/IP et non pas le modèle OSI
- il est simplifié, notamment en supprimant les redondances dans les informations et les fonctionnalités peu utilisées
- il utilise des chaînes de caractères pour représenter ses données plutôt qu'une syntaxe complexe comme ASN.1 (*Abstract Syntax Notation 1*)
- il est basé sur le modèle client / serveur et est donc reconnu comme un service de ce modèle, au même titre que les services d'impression, de serveur de fichiers ou encore de courrier électronique

[24] L'historique de LDAP est présenté dans de nombreux documents, dont cette partie en est un résumé.

Pour qu'un client accède aux données de l'annuaire, le service X.500 doit comprendre les messages LDAP expédiés par le client. Or le serveur X.500 ne peut être interrogé que via DAP et le modèle OSI. Ce problème a été résolu par l'introduction d'un serveur passerelle, ou encore proxy, permettant le passage de messages LDAP sous TCP/IP à des messages DAP sous OSI. La figure ci-dessous représente une telle situation.

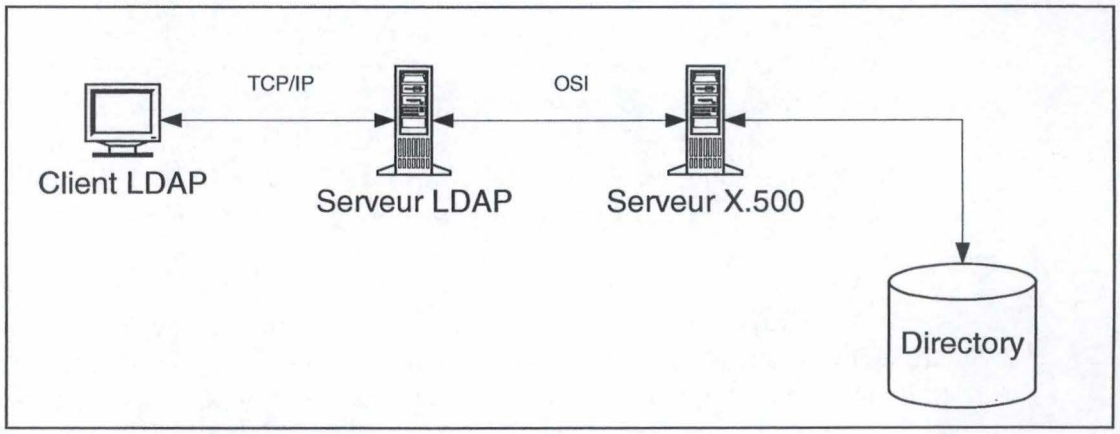

Figure 11. LDAP - PROXY LDAP

Suite au succès du protocole LDAP, les serveurs passerelles ont évolué pour accéder directement à l'information et ce sans recourir au serveur X.500. On parle alors de serveur LDAP en tant que service d'annuaire.

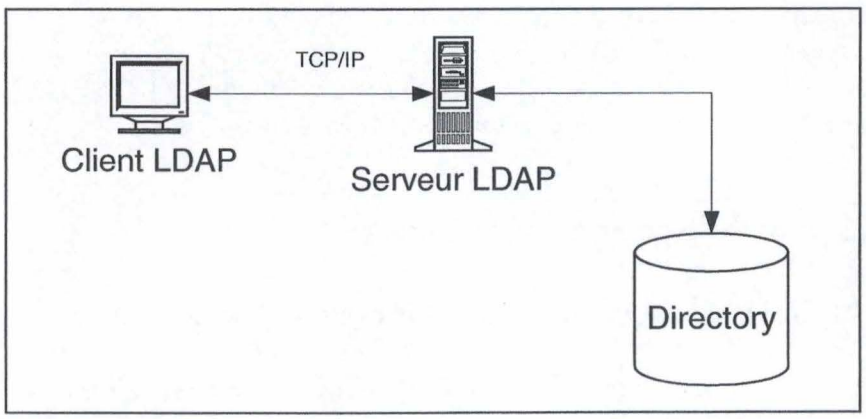

Figure 12. LDAP - SERVEUR LDAP

Bien que LDAP soit un protocole, on désigne souvent les serveurs supportant ce protocole comme "serveur LDAP". Ces derniers comportent les éléments suivants :

- le protocole en lui-même définissant les opérations, l'authentification et l'échange des données,
- une série de méthodes regroupées en un API (*Application Protocol Interface*) est utilisée pour la réalisation d'application,
- un système d'URL (*Uniform Resource Locator*) permettant l'interrogation d'un service d'annuaire au travers d'un navigateur standard par l'utilisation d'URL du type "ldap://url",
- un format de données appelé LDIF (*LDAP Data Interchange Format*) permettant de créer, modifier et supprimer les entrées d'un annuaire à partir de fichier texte.

3.4Concepts et architecture

3.4.1 Concepts de base[25]

Tous les concepts de base de LDAP sont repris dans les différents RFC. Néanmoins, certains spécialistes ont documenté et vulgarisé ces notions.

L'unité de base en LDAP est ce que l'on appelle une entrée ("entry"). Une entrée peut représenter une personne, un serveur ou encore une organisation. Chaque entrée possède une série d'attributs, un attribut étant constitué d'un nom l'identifiant et d'une série de valeurs.

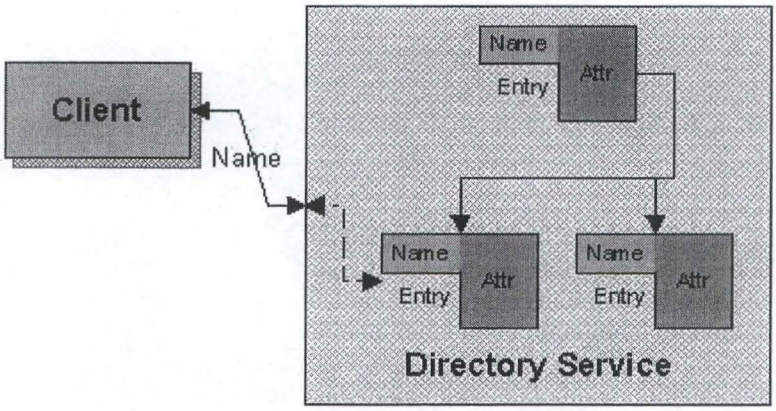

Figure 13. LDAP - SERVICE DE NOMS

Les entrées sont contenues dans une structure hiérarchique appelée "directory information tree (DIT)" qui forme la structure de base de LDAP. Chaque feuille de l'arbre est alors une entrée ("entry"), la première de ces entrées étant appelée "root entry". Cette dernière est purement conceptuelle et n'est donc pas représentée dans le schéma.

Chaque entrée est identifiée dans l'arbre à partir de son Distinguished Name (DN). Le DN, qui est unique dans l'arbre, montre la relation de l'entrée avec le reste de l'arbre. On peut le comparer avec le chemin menant à un fichier sur un disque. La partie la plus à gauche du DN se nomme "relative distinguished name (RDN)" et est constituée d'une suite de paires attribut/valeur.

Ainsi, pour représenter un étudiant de la licence à horaire décalé des FUNDP, on utilise les données suivantes :

- L'étudiant en question réalise son mémoire et fait partie de la section lihd-m
- La section lihd-m fait partie de la licence en informatique à horaire décalé de l'institut d'informatique, institut faisant partie des Facultés Universitaire Notre Dame de la Paix à Namur, Belgique.

[25] Citons par exemple Wang Y., Janvier 1998 ou encore Tyagi S., Mars 2000

La construction de l'arbre se fait de l'entité la plus important (le pays) pour se terminer sur l'entité la plus petite, à savoir l'étudiant.

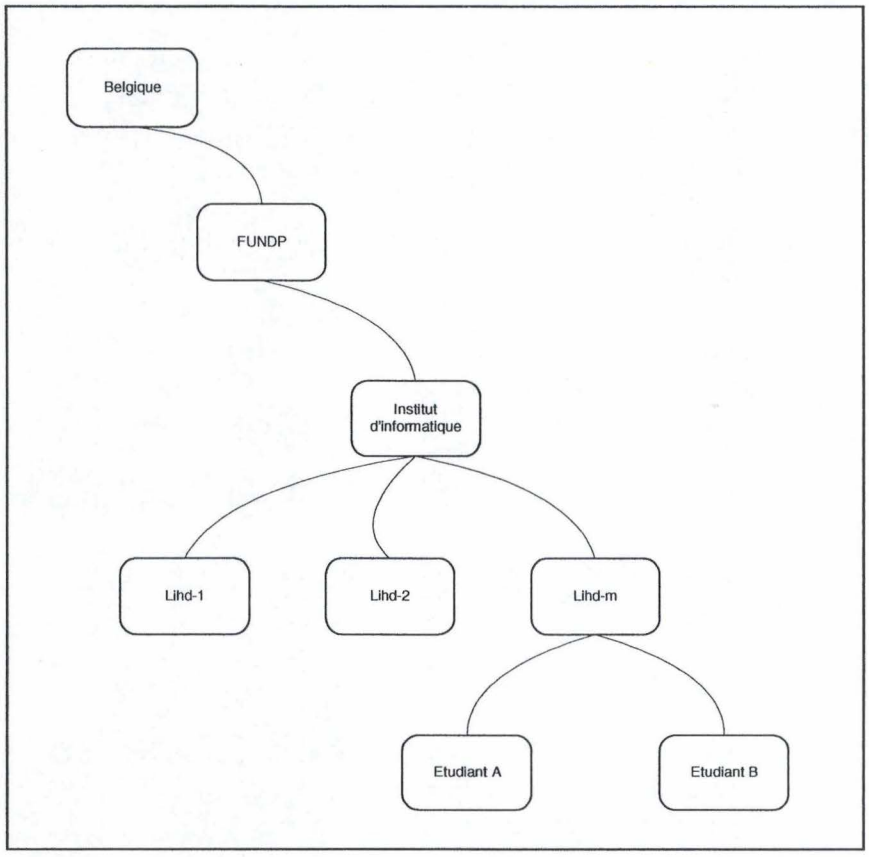

Figure 14. LDAP - ARBRE LIHD-M

Le DN se définit comme le parcours réalisé pour arriver à l'entrée, avec la particularité qu'il se construit de droite à gauche en débutant par la racine de l'arbre. Il vaut donc *"Etudiant A , Lihd-M , Institut d'informatique, FUNDP , Belgique"*.

Les quelques notions reprises ci-dessus n'expliquent pas quel est le modèle logique des données, comment l'annuaire est organisé ni quelles opérations sont possibles. Une approche intéressante a été développée par des ingénieurs d'IBM. Selon eux, ***LDAP peut être vu comme un ensemble de quatre modèles***[26] :

- ***modèle des données*** : il décrit la structure de l'information que l'on trouve dans un annuaire LDAP
- ***modèle d'adressage*** : il décrit comment l'information est organisée et identifiée
- ***modèle fonctionnel*** : il décrit les opérations que l'on peut effectuer
- ***modèle de sécurité*** : il décrit comment les données sont protégées

[26] Johner H., Brown L., Hinner F.-S., Reis W., Westman J., 1998, p.24

3.4.2 Modèle des données

Comme cela a été introduit précédemment, l'unité d'information de base est une entrée de l'arbre. Chaque entrée est composée d'une série d'attributs, chaque attribut pouvant contenir un certain type de données.

Un attribut, même multivalué, ne peut évidemment contenir qu'un seul type de données dont la représentation est fixée par une syntaxe. Par exemple, un attribut de type 'numéro bancaire' pourra accepter des chiffres en plus du tiret et devra respecter une certaine syntaxe définissant le format du numéro bancaire.

A ces définitions viennent s'ajouter les règles à appliquer lors des recherches et autres opérations, à savoir :

- ordre lexicographique
- caractère alphanumérique ou non
- respect de la casse (majuscule/minuscule), des espaces et autres caractères particuliers
- des contraintes comme la taille limite de la valeur d'un attribut

Toutes ces informations sont reprises dans le schéma des données. Ce schéma est divisé en quatre sections :

- *"class definition"* :

  Cette section définit les types d'objets, ou classes d'objets que l'on peut trouver dans l'annuaire. Pour chaque objet, on définit les attributs qui sont obligatoires et ceux qui sont optionnels.

  Le plus intéressant est que cette définition reprend ***deux concepts des langages orientés objets, à savoir l'héritage et la notion d'objet dérivé***. Il est donc possible de définir un objet dérivant d'un autre, qui hérite des attributs du père et de leurs particularités, et d'ajouter de nouveaux attributs, obligatoires ou optionnels.

  Le mécanisme de dérivation s'exprime au travers d'un attribut spécial obligatoire nommé "objectclass". Cet attribut multivalué reprend la liste du ou des pères de l'objet et détermine indirectement, via le mécanisme d'héritage, les attributs obligatoires ou optionnels hérités des pères. Il contient au moins le nom de la classe de base de tout annuaire, à savoir la classe "top". Cette dernière définit justement l'attribut obligatoire "objectclass".

Voici un exemple de classes standards reprises dans les implémentations actuelles, permettant dans ce cas de représenter une organisation :

Classe	Description
top	la classe mère de toute autre classe
country	classe définissant un pays
organisation	classe définissant une organisation
organizational Unit	classe définissant un département ou un service d'une organisation
inetOrgPerson	classe définissant un membre du personnel d'une organisation
organizational Role	classe définissant le rôle joué par un ou plusieurs membres d'une organisation

- *"attribute definition"* :

Cette section reprend la définition des attributs, à savoir le type de données qu'ils représentent tels que données binaires, chaînes de caractères, entiers, ... On détermine aussi quelle syntaxe utiliser pour cet attribut, savoir si le champ est multivalué ou nom et s'il faut l'indexer.

De nombreux attributs LDAP, sont en fait des mnémoniques, dont voici quelques exemples :

Attribut	Description
c	pays
o	organisation
ou	service (d'une organisation)
cn	nom commun d'une personne, d'un rôle
	...
mail	adresse mail

- *"syntax définition"* :

Cette section définit la représentation des données à savoir les règles particulières définissant la valeur de l'attribut. Par exemple, on trouve des syntaxes pour les comptes bancaires, les numéros de téléphone ou encore les adresses e-mail.

- *"matching rule définition"* :

Cette section définit les règles à appliquer lors des recherches, comme par exemple le respect de la casse.

Toutes les définitions reprises dans le schéma peuvent être manipulées par l'administrateur de l'annuaire, à l'exception des objets servant de base au système comme la classe "top". Il est donc possible de définir son propre modèle des données ayant pour structure le schéma de base de l'annuaire.

La dernière version de LDAP (Ldap v3) permet de ***retourner les informations concernant le serveur lui-même, ce qui inclus le modèle des données*** et donc les quatre sections décrites ci-dessus.

3.4.3 Modèle d'adressage

Le modèle d'adressage définit comment les données sont identifiées et organisées.

L'identification :

Le DN, définit comme le parcours de l'arbre pour arriver à l'objet désiré, est la clé d'accès de l'annuaire. Il est constitué d'une séquence de "relative distinguished name" (RDN), les RDN étant séparés entre eux par une virgule. Un RDN n'est autre que la partie la plus à gauche du DN, à savoir la dénomination de l'entrée. Le DN de l'entrée se construit donc en additionnant le RDN au DN de l'entrée père.

Si l'on reprend l'exemple de l'étudiant en licence à horaire décalé, le RDN extrait de *"Etudiant A , Lihd-M , Institut d'informatique, FUNDP , Belgique"* équivaut à *"Etudiant A"*, le DN du père valant *"Lihd-M , Institut d'informatique, FUNDP , Belgique"*.

Chaque RDN provient des attributs définis de l'entrée. Dans la plupart des cas, il équivaut au nom de l'attribut, suivi du signe égal et de la valeur de l'attribut. Comme LDAP utilise toute une série de mnémoniques pour nommer les attributs, le DN est construit selon la séquence des RDN suivants :

- "cn=Etudiant A" représente l'étudiant
- "ou=lihd-m" représente la licence à horaire décalée, vue comme une section
- "ou=institut d'informatique" représente l'institut d'informatique, vu comme un département
- "o=fundp" représente les facultés vues comme une organisation
- "c=be" représente la Belgique.

Le DN équivaut à "cn=Etudiant A, ou=lihd-m, ou=institut d'informatique, o=fundp, c=be".

Basé sur le même exemple, le DN représentant les Facultés Universitaires Notre-Dame de la Paix équivaut à "o=fundp, c=be", son RDN étant "o=fundp" et le DN du père "c=be".

La syntaxe exacte d'un DN est reprise en annexe à titre d'information.

L'organisation :

Les données sont organisées dans le DIT selon leur DN. Par exemple, le DIT correspondant à l'exemple de l'étudiant à horaire décalé pourrait être celui-ci :

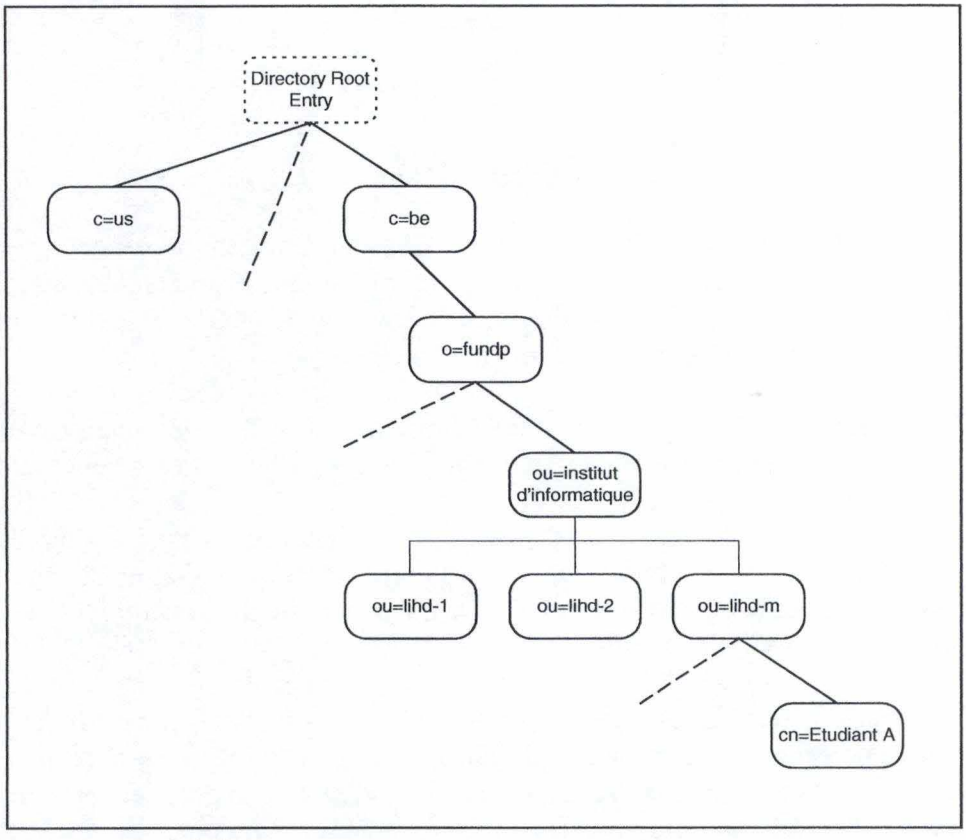

Figure 15. LDAP - EXEMPLE D'UN DIT : LIHD-M

Il est parfois difficile de mettre en place un DIT cohérent et correct, surtout lorsque la structure s'avère complexe. Typiquement, on rencontre deux types de problèmes :

- ***l'annuaire est distribué*** sur plusieurs serveurs, pour des raisons organisationnelles ou techniques
- ***une entrée du DIT doit être représentée à deux endroits différents***, ce qui peut se justifier par exemple lorsqu'une personne joue un ou plusieurs rôles dans des services différents ou bien doit être déplacée, ce qui modifie son DN, mais l'ancienne entrée ne peut être supprimée afin de maintenir une compatibilité.

Les ***références*** sont des objets particuliers qui solutionnent le premier problème en indiquant que l'entrée en question n'est pas stockée sur ce serveur. Un attribut de cette entrée indique d'ailleurs l'URL LDAP du serveur à interroger. Les annuaires n'ont pas pour obligation de suivre de tel lien, ce qui accroît leur performance mais oblige les clients à suivre eux-mêmes ces liens. Afin de limiter la charge du client, ***la plupart des API LDAP*** sont programmables pour qu'elles ***suivent automatiquement les liens***, et ce de façon tout à fait transparente pour le client.

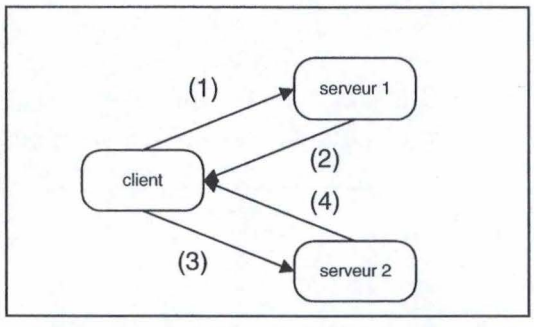

Figure 16. LDAP - REFERENCE SUIVIE PAR UN CLIENT LDAP

La figure ci-dessus montre une telle situation. Le client demande une série d'information au premier serveur (1). Le serveur revoit les résultats mais une des entrées est une référence (2). L'API Ladp prend en charge l'interrogation du deuxième serveur (3). Le deuxième serveur retourne l'information au client (4).

Certains vendeurs permettent la résolution de tels liens, le travail est donc pris en charge par le serveur. Cette fonctionnalité ne fait pas partie de LDAP v.3

Les ***suffixes*** permettent de connaître les branches du DIT gérées par l'annuaire. Un suffixe est donc l'entrée la plus haute de l'arbre que stocke l'annuaire. Chaque entrée de l'annuaire se termine donc par ce suffixe, ce qui se justifie aisément vu que les entrées de haut niveau sont toujours à la fin du DN.

Pour illustrer l'utilisation des références et des suffixes, on modifie l'exemple développé précédemment en indiquant que les informations relatives à la licence à horaire décalé sont stockées sur un autre serveur. Une des entrées du premier serveur, par exemple la lihd-m est en fait une référence vers un deuxième serveur contenant les étudiants réalisant leur mémoire.

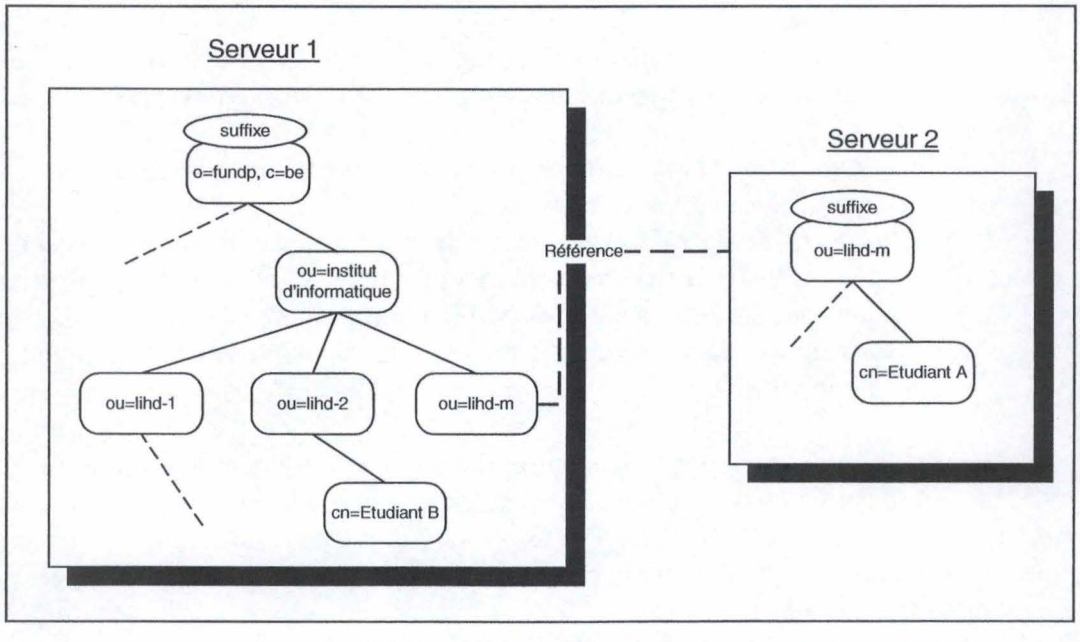

Figure 17. LDAP - UTILISATION DES REFERENCES ET DES SUFFIXES

Dans le cas où il est nécessaire qu'une entrée du DIT se trouve à 2 endroits différents dans celui-ci, l'utilisation d'***alias*** s'avère utile. ***Un alias est un type d'objet particulier qui indique que l'entrée en question n'est qu'une image d'une autre entrée du DIT.***

Propriétés d'adressage d'un annuaire

Selon LDAP v.3, le service d'annuaire doit fournir toute une série d'informations le concernant. Ces informations, obtenues en passant au serveur un DN vide (chaîne de caractères vide), sont les suivantes :

- les suffixes gérés par le serveur
- le DN d'une entrée spéciale permettant d'obtenir le schéma des données
- la ou les versions LDAP supportées
- la liste des opérations et contrôles étendus supportés
- le liste de serveurs LDAP alternatifs
- la liste des mécanismes de sécurité supportés

3.4.4 Modèle fonctionnel

En tant que protocole, LDAP définit de manière indépendante du langage les opérations réalisables sur l'annuaire. Il y a quatre grandes familles d'opérations :

- les mise à jour de l'annuaire via l'ajout, la modification et la suppression des entrées
- les opérations d'authentification permettant d'identifier le client et de déterminer les opérations autorisées
- les recherches et comparaisons dans l'annuaire
- Les contrôles et opérations étendues

Les mises à jour :

Les opérations de mise à jour concernent le contenu de l'annuaire et sont les suivantes :

Ajout	insère une nouvelle entrée
Suppression	supprime une entrée existante à condition qu'elle soit la dernière de sa branche. Les suppressions en cascade ne sont donc pas autorisées, de même les alias ne sont pas mis à jour ou résolus lors d'une suppression
Modification d'une entrée	modifie, ajoute ou supprime un attribut de l'entrée
Modification du RDN	permet de modifier le RDN et donc de déplacer une partie de l'arbre. Cette opération ne permet pas de déplacer une partie de l'arbre d'un serveur à un autre

L'authentification :

En s'authentifiant on détermine ainsi le niveau de sécurité des opérations. Les mécanismes d'authentification sont détaillés dans le modèle de sécurité (cf. 3.4.5 Modèle Sécurité).

Les recherches et comparaisons :

Ces opérations sont de loin les plus complexes. Il n'y a aucune distinction entre les opérations de recherche dans l'arbre, l'obtention d'une liste d'entrées ou bien la récupération des attributs d'une entrée. La recherche est composée des éléments suivants :

- la base : il s'agit du DN à partir duquel la recherche va débuter
- la portée ("scope") : détermine s'il s'agit d'obtenir les attributs de la base, d'obtenir la liste des entrées situées directement sous la base ou bien d'obtenir toutes entrées de l'arbre débutant au DN servant de base.
- les attributs recherchés : permet de spécifier la liste des attributs à rechercher
- le filtre de recherche : le filtre de recherche détermine les critères qu'une entrée doit respecter pour faire partie des résultats. La base du filtre se compose d'un attribut, d'un opérateur et de la valeur recherchée. Les opérateurs suivants peuvent composer un filtre :

Opérateur	Description
=	Retourne les entrées dont l'attribut possède la valeur recherchée
>=	Retourne les entrées dont la valeur des attributs est supérieure ou égale à la valeur recherchée
<=	Retourne les entrées dont la valeur des attributs est inférieure ou égale à la valeur recherchée
=*	Retourne les entrées ayant une valeur pour l'attribut spécifié
~=	Retourne les entrées dont la valeur de l'attribut approche la valeur spécifiée

Il est possible de combiner les triplets attributs/opérateurs/valeurs pour former un filtre plus complexe. On utilise alors les opérateurs booléens suivants :

Opérateur booléen	Description
&	Retourne les entrées satisfaisant à tous les critères
|	Retourne les entrées satisfaisant à au moins un des critères
!	Retourne les entrées pour lesquelles le filtre n'est pas vrai.

Si le caractère '*' est présent dans un filtre, il prend en fait n'importe quelle valeur.

Voici quelques exemples de recherches basés sur notre étudiant en licence à horaire décalé :

1. Recherche de tous les étudiants de la licence à horaire décalé préparant leur mémoire :

   Base DN : "ou=lihd-m, ou=institut d'informatique, o=fundp, c=be"
   Scope : Toutes entrées à partir du DN
   Attributs recherchés : tous
   *Filtre : cn=**
   Limite : aucune

2. Recherche des adresses e-mails des étudiants de la licence à horaire décalé préparant leur mémoire :

   Base DN : "ou=lihd-m, ou=institut d'informatique, o=fundp, c=be"
   Scope : Toutes entrées à partir du DN
   Attributs recherchés : [mail]
   *Filtre : cn=**
   Limite : aucune

3. Recherche des étudiants dont la première lettre du nom est comprise entre D et M :

   Base DN : "ou=lihd-m, ou=institut d'informatique, o=fundp, c=be"
   Scope : Toutes entrées à partir du DN
   Attributs recherchés : tous
   Filtre : cn=(| (cn>=D) (cn<=M*))*
   Limite : aucune

- les limites : il est possible de limiter les recherches, notamment le temps de recherche et le nombre des données maximums recherchées.

La comparaison permet de déterminer si une entrée a une certaine valeur pour un attribut. L'avantage de la comparaison sur la recherche réside dans le fait que la comparaison distingue le cas ou l'entrée ne contient pas la valeur recherchée et où l'entrée n'existe pas.

Le comportement de la recherche et de la comparaison peut être modifié par les éléments suivants :

- les alias : il est possible d'obtenir les informations sur l'objet alias en lui-même ou bien d'obtenir les informations de l'objet caché derrière l'alias.

- les références : les références ne sont pas résolues par le serveur mais peuvent être suivies par les libraires (API) LDAP ou bien signalées au client.

Les contrôles et opérations étendues :

Ces opérations permettent d'étendre le protocole sans le modifier. Les contrôles permettent de modifier une opération existante tandis que les opérations étendues ajoutent de nouvelles opérations au protocole. Ces informations sont obtenues en interrogeant l'annuaire sur ses propriétés d'adressage.

3.4.5 Modèle Sécurité

Par défaut, toute connexion à un serveur LDAP se fait de façon anonyme. Il n'est donc pas nécessaire de s'authentifier pour interroger un annuaire. Néanmoins, plusieurs mécanismes ont été mis en place afin d'assurer l'authentification, l'intégrité et la confidentialité des données.

Comme cela a été introduit précédemment, une session peut être ouverte avec le service d'annuaire. Il y a trois façons de débuter une session :

- pas d'authentification : le serveur crée une session dite "anonyme"
- authentification simple : le client soumet un DN et un mot de passe non chiffré. Certains vendeurs utilisent le codage en Base64 pour les mots de passe. Ce codage provient du format MIME (*Multipurpose Internet Mail Extensions*) définit par le RFC 1521 mais ne fait pas partie du standard LDAP V.3
- SASL (*Simple Authentification and Security Layer*) : LDAP V.3 intègre ce mécanisme d'authentification. Il est déjà utilisé dans d'autres protocoles, comme SMTP (*Simple Mail Transfert Protocol*). Il comprend trois paramètres :
  - un DN : le DN de l'entrée qui déterminera les droit d'accès
  - mécanisme : il s'agit du nom de la méthode à utiliser pour sécuriser la communication. Plusieurs mécanismes sont supportés, dont KEBEROS, S/Key, ANONYMOUS et EXTERNAL. Ce dernier reprend les communications de types SSL (*Secure Socket Layer*).
  - "crédentials" : il s'agit de données permettant d'identifier le DN. Le mécanisme utilisé pour la sécurisation de la communication détermine le contenu de ce paramètre.

En plus d'une ouverture de session, certains annuaires permettent de spécifier des autorisations pour chaque entrée de l'annuaire. Ce mécanisme des ACL (*Access Control List*), qui ne fait pas partie du standard LDAP V.3, détermine les opérations de lecture, écriture et de suppression d'une entrée pour chaque utilisateur ou groupe d'utilisateurs. Il est en cours de standardisation.

3.5Modélisation des organisations

3.5.1 Dans les grandes lignes

La chose la plus importante à retenir lorsque l'on veut mettre en place un annuaire, c'est qu'il doit ***résister aux changements***. L'annuaire est en effet amené à évoluer, par l'ajout de nouveaux éléments, mais aussi par la suppression ou le déplacement d'objets existants. Il est alors impératif que ces modifications n'entravent pas la bonne exécution des applications utilisant l'annuaire ou bien la compréhension que les utilisateurs ont de celui-ci.

Voici quelques considérations[27] qui s'imposent à chaque planification d'un annuaire :

Quelles données doit-on stocker dans l'annuaire et comment les organiser ?

- il est nécessaire d'identifier les personnes de l'organisation ayant un contrôle sur le contenu de ces données
- si les données font parties d'un ou de plusieurs systèmes d'informations, il faut prévoir un mécanisme d'échange entre l'annuaire et ces systèmes

→ ***Modèle des données***

L'annuaire sera-t-il un annuaire distribué ?

- il est nécessaire de déterminer les ***suffixes*** (donc les branches du DIT) supportés par chaque serveur ainsi que l'endroit où placer les ***références***.

→ ***Modèle d'adressage***

Comment gérer les données et assurer leur intégrité et confidentialité ?

- il est nécessaire de déterminer les personnes ayant la charge de valider les données exposées dans l'annuaire
- il est nécessaire de déterminer les personnes ayant l'autorité pour autoriser ou non l'accès à certaines données et donc de définir les droits d'accès pour chaque donnée.

→ ***Sécurité et politique d'accès***

D'autres types de considérations sont aussi à prendre en compte mais dépendent plus de l'utilisation ou de l'environnement du client :

- comment les clients vont-ils accéder aux données ?

[27] Ces considérations sont reprises dans la plupart des publications traitant de la modélisation des données d'un annuaire électronique. Johner H., Brown L., Hinner F.-S., Reis W., Westman J., 1998 ou encore Netscape Communications Corporation, 1999

- l'annuaire doit-il être disponible à tout moment et comment survenir aux pannes ? Faut-il prévoir un mécanisme de réplication de données ?

- le système en général, c'est-à-dire les serveurs et le réseau, est-il suffisant pour supporter l'utilisation de l'annuaire ?

→ Design Physique

3.5.2 Définition du modèle des données

Le modèle des données doit provenir de l'analyse des informations que l'on veut y stocker, à savoir :

- quels types de données sont utilisés couramment par les applications ?
- la structure organisationnelle provient-elle d'un système d'exploitation ou d'une application propriétaire ?

Le modèle des données standard de LDAP suffit-il à modéliser tous les types de données identifiés ? Si cela n'est pas le cas, il est ***conseillé d'étendre le schéma standard*** en modifiant les quatre sections le composant : les classes, les attributs, les syntaxes et les "matching rules" . ***Inclure ses propres objets permet de préserver le schéma de base***, qui peut en effet être utilisé pour d'autres applications.

La cohérence a aussi beaucoup d'importance. Si un attribut ou un objet est utilisé pour stocker un type d'information, il est important de maintenir le rôle de cet attribut ou objet au travers du DIT.

Enfin, si les données proviennent d'un autre système ou si un autre système doit y accéder, il faut prévoir un mécanisme de mise à jour automatique.

3.5.3 Définition du modèle d'adressage

L'identification a pour but de fournir une manière unique de localiser une entrée dans le DIT. La manière de ***construire l'identification, donc le DN, doit être le plus intuitif possible*** afin de faciliter la recherche d'information et l'administration du DIT.

Cela est particulièrement vrai si l'information stockée concerne des personnes. Il n'est pas rare que deux personnes portent le même nom. Habituellement, l'attribut "cn" (common name) est utilisé dans le DN afin d'identifier une personne. Si deux personnes portant le même nom appartiennent au même service, cette manière de construire le DN ne permet pas de modéliser ce cas de figure. Une autre option est l'utilisation de l'attribut "uid" (user ID) qui est l'équivalent du "login". La valeur de cet attribut est habituellement unique dans tout l'annuaire.

Pour l'organisation des entrées dans le DIT, il est courant de suivre un schéma organisationnel où ***les objets sont organisés selon leur importance***. Par exemple, les pays se trouvent au sommet de l'arbre, suivis par les organisations nationales et les régions, les provinces, ... Bien après cela, on trouve les personnes à proprement parler, le service dans lequel elles évoluent et le rôle qu'elles jouent dans leur organisation.

Si, pour des raisons de compatibilité avec des applications, il est impossible de déplacer une entrée, l'utilisation des alias est alors conseillée. Cela garantit une certaine compatibilité avec l'ancien DIT. L'alias est à utiliser avec précaution car de telles références sont à sens unique et LDAP ne fournit aucun support afin de mettre à jour ces références. Un problème pourrait survenir si l'entrée référencée venait à être supprimée.

La planification des ***références*** et des ***suffixes*** est une chose très importante. La structure organisationnelle supporte parfois naturellement les références, notamment pour les multinationales. Il est parfois aussi utile d'isoler une partie du DIT sur un autre serveur car celle-ci est plus souvent accédée que le reste de l'arbre.

Si le DIT est distribué sur plusieurs annuaires, deux problèmes peuvent survenir :

- il n'est pas certain que le modèle des données soit identique d'un serveur à l'autre
- les droits d'accès sont peut-être différents d'un serveur à l'autre

La planification des références doit donc être très soignée

3.5.4 Définition de la sécurité et de la politique d'accès

La sécurité et la politique d'accès doivent être assez efficace afin de garantir la confidentialité et l'intégrité des données.

A moins que les données ne soient sensibles, l'authentification simple sera choisie. L'authentification simple nécessite un minimum d'administration, notamment pour la gestion des mots de passe.

L'utilisation de SASL, surtout au travers de SSL, est utile pour la communication de serveur à serveur ou pour garantir l'accès à un annuaire dont les données sont sensibles. Ce mécanisme peut se révéler intéressant pour une utilisation au travers d'Internet. LDAP prévoit d'ailleurs un attribut permettant de stocker la clé publique d'un utilisateur.

La majorité du DIT est souvent accessible en lecture, la mise en place d'ACL permet de protéger une partie du DIT ou de ne dévoiler que certains attributs. La mise à jour ou la suppression sera contrôlée au travers des ACLs.

3.5.5 Définition du design physique

Le design physique est abordé à titre informatif afin d'informer le lecteur :

- la disponibilité :

Lorsque le service d'annuaire est un élément critique d'une application, il est nécessaire de maintenir le niveau de service. LDAP fournit deux éléments pour solutionner ce problème :

- la découpe du DIT et le stockage de chaque partie sur des serveurs différents
- la réplication des données d'un annuaire maître vers un annuaire esclave situé sur une autre machine

Il est aussi évident que le dimensionnement de la machine (CPU, RAM, ...) joue un rôle essentiel dans la disponibilité du service.

➢ la facilité d'administration :

La plupart des vendeurs fournissent une interface d'administration dite conviviale. Le format LDIF peut aussi servir à administrer le service d'annuaire

→ Ces éléments ne font pas partie du standard LDAP V.3. Il est donc conseillé de s'adresser à chaque vendeur afin de déterminer le niveau de service que peut fournir sa solution.

3.6Exemples de modélisation

Deux exemples vont servir de base à l'illustration des concepts et du développement d'une solution utilisant les annuaires. Le premier exemple décrit un annuaire représentant les administrations belges, tandis que le second prend l'exemple d'une administration utilisant son annuaire afin d'aider ses administrés dans leurs recherches d'informations.

3.6.1 Annuaire électronique fédéral

Cet exemple développe l'utilisation d'un annuaire afin de représenter l'ensemble des administrations belges. Les caractéristiques de cet annuaire sont les suivantes :

- l'annuaire mettra en place une structure hiérarchique reprenant les diverses entités du pays (fédéral, régional et communautaire), leurs départements et leur personnel
- la racine de cette structure sera le gouvernement fédéral
- chaque entité déploiera un annuaire et sera responsable des informations la concernant

Comment procéder ?

1. Déterminer les informations à introduire dans l'annuaire. Dans cet exemple, les informations concernent les organisations, les départements, les services et le personnel. La plupart des annuaires fournissent des objets modélisant toutes ces informations.

2. Déterminer la structure de l'annuaire. La mise en place sera de type "top - down", c'est-à-dire que les éléments apparaissent dans l'ordre suivant : pays, organisation, départements, services et personnel.

3. Déterminer les suffixes et les emplacements pour les références.

   - Le premier des suffixes n'est autre que l'indicatif du pays, à savoir *"c=be"*. L'annuaire du gouvernement fédéral doit reprendre, en plus des ministères fédéraux, les références vers les autres entités du pays, à savoir les trois régions et les trois communautés. Les suffixes supportés par l'annuaire fédéral sont *"c=be"* et *"o=gouvernement fédéral, c=be"*.
   - Les autres suffixes correspondent aux références planifiées dans l'annuaire du gouvernement fédéral. Par exemple, pour le Région Wallonne, il sera équivalent à *"o=Région Wallonne, c=be"*.

4. La planification d'autres références et suffixes, la mise en place d'une structure hiérarchique particulière ou l'utilisation d'alias sont à la discrétion de chaque entité.

5. La lecture de l'annuaire doit être garantie pour tous et de façon anonyme.

La figure ci-dessous est une solution possible pour l'annuaire fédéral :

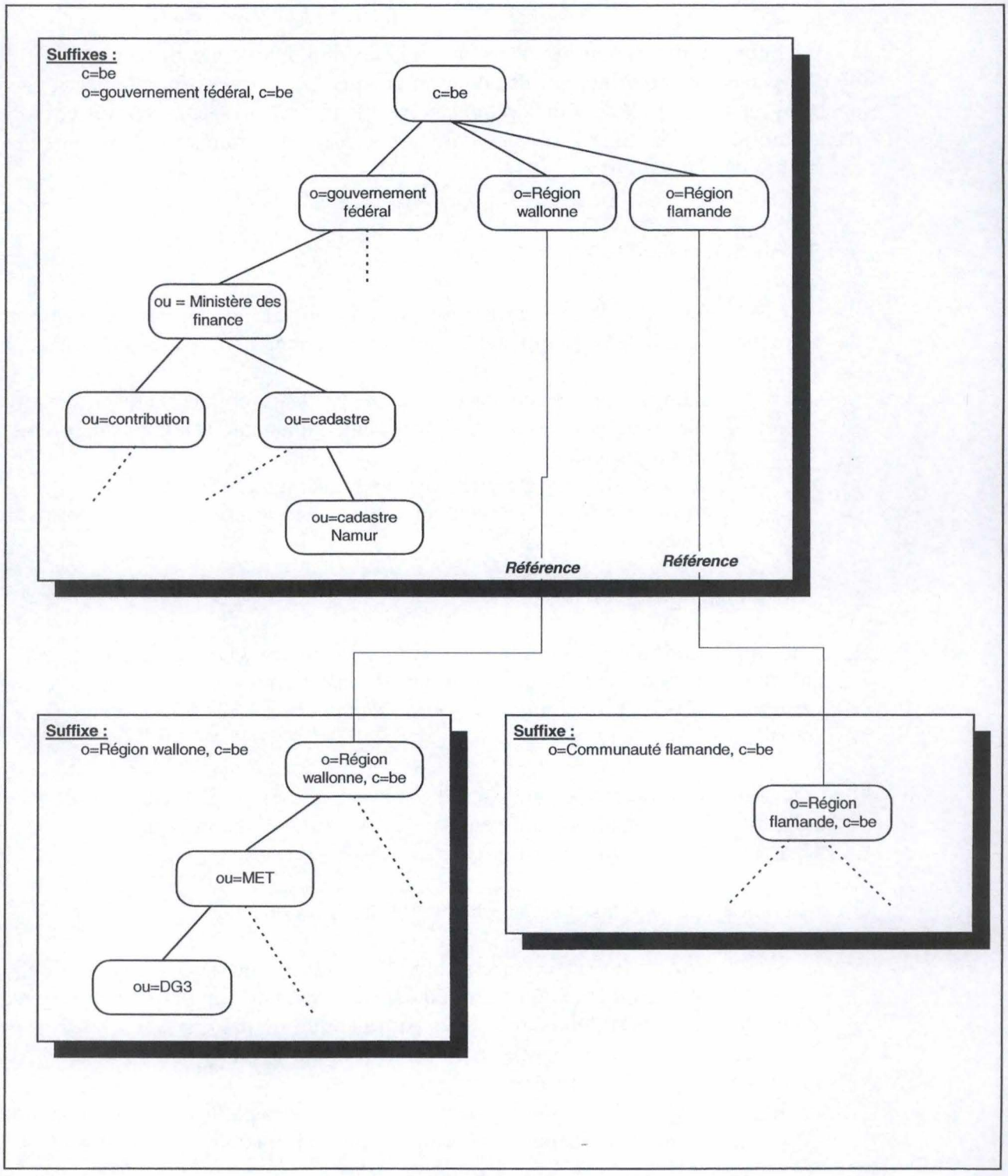

Figure 18. LDAP - EXEMPLE D'UN ANNUAIRE FEDERAL

3.6.2 Annuaire en tant que support à un système informationnel

Cet exemple développe un annuaire utilisé comme support à un système informationnel. En plus de stocker la représentation organisationnelle de l'administration, l'annuaire va servir à aider le citoyen dans sa recherche de l'information en reprenant une seconde structure organisée en thèmes.

On peut comparer cette structure aux FAQs (Frequently Ask Question). Par exemple, les thèmes fréquemment rencontrés dans une administration communale concernent l'état civil (mariage, décès, ...), les permis de bâtir, ...

Chaque thème reprend un descriptif, la procédure à suivre, les documents nécessaires, les coordonnées et les heures d'ouverture du service assurant le traitement du thème ainsi que la ou les personnes de contact.

Comment procéder ?

1. Déterminer les informations à introduire dans l'annuaire. La représentation organisationnelle est une structure hiérarchique classique qui se modélise à partir des objets fournis en standard par chaque annuaire. Puisqu'il n'y a théoriquement aucun objet standard censé modéliser un thème, on crée un nouvel objet détaillant le thème.

2. Déterminer la structure de l'annuaire. La mise en place sera de type "top - down" pour la représentation organisationnelle de l'administration. Les thèmes seront regroupés sous une entrée commune. Les services et le personnel étant déjà représenté, il ne sera pas nécessaire de redéfinir les informations les concernant. L'utilisation d'alias facilite d'ailleurs le lien entre le thème, le service et les personnes de contact.

3. Déterminer les suffixes et les emplacements pour les références. Le seul suffixe supporter par cet annuaire est celui utilisé par l'administration, comme par exemple *"o=Ville de Namur, c=be"*.

4. Le public a accès aux deux structures.

La figure ci-dessous est une solution possible pour l'annuaire à thème :

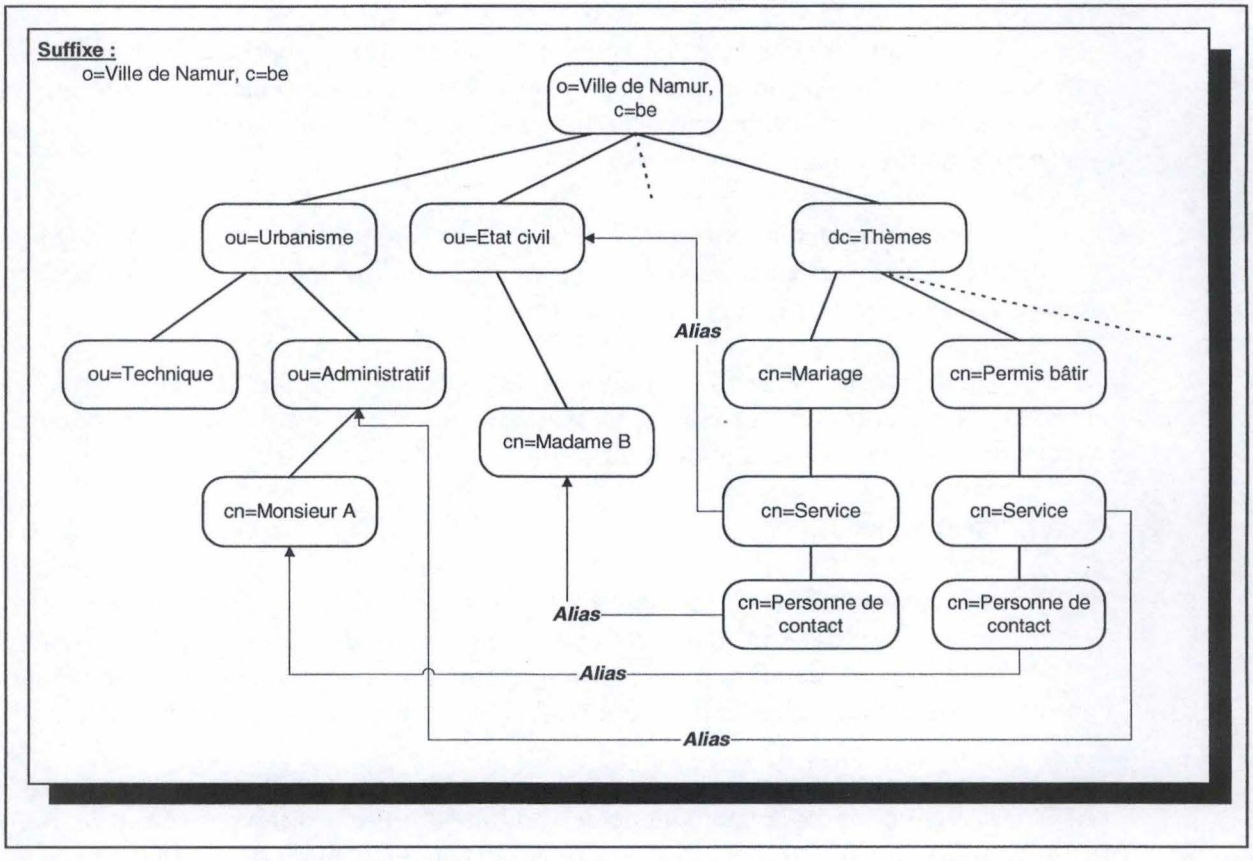

Figure 19. LDAP - EXEMPLE D'UN ANNUAIRE EN SUPPORT D'UN SYSTEME INFORMATIONNEL

3.7Utilisation des annuaires électroniques dans AdmiPRO

L'utilisation dans AdmiPRO des annuaires électroniques est le résultat d'une veille technologique dédiée à la représentation organisationnelle dans les systèmes d'informations. L'implémentation originale mise en place suit le processus suivant :

- étude des besoins
- choix techniques
- modélisation organisationnelle
- réalisation technique

L'étude des besoins se base à la fois sur le cahier des spécifications et sur l'expérience du projet pilote PBFlow.

Les choix techniques effectués doivent intégrer les principes et concepts de la représentation organisationnelle au travers de LDAP. De plus, ce choix doit être compatible avec les choix techniques faits précédemment dans AdmiPRO (cf. 2.5 Technologies utilisées).

La modélisation des organisations dans AdmiPRO suit les grands principes développés précédemment (cf. 3.5 Modélisation des organisations). La découpe réalisée est composée des trois premiers modèles à savoir le modèle des données, le modèle d'adressage et le modèle de la sécurité et politique d'accès. Le design physique ne sera pas abordé car il dépend essentiellement de l'environnement d'exploitation et non des fonctionnalités du logiciel AdmiPRO. Voici, dans les grandes lignes, les consignes mises en place :

- le modèle des données préserve les objets basiques de l'annuaire et les mécanismes d'héritage sont utilisés.
- le modèle d'adressage fera appel aux références et aux alias. La structure de l'arbre organisationnel reprendra les structures des départements et services des entités.
- le modèle de la sécurité et politique d'accès se base sur l'authentification et l'utilisation des ACLs.

Enfin, la réalisation technique décrit l'architecture logicielle mise en place. Pour des raisons de confidentialité, le code développé ne fait pas partie de ce document.

3.7.1 Les besoins

Afin d'intégrer une organisation, le logiciel AdmiPro doit répondre aux besoins suivants :

- assurer la représentation de la structure organisationnelle
- assurer la représentation des compétences organisationnelles (statuts & compétences)

Ces besoins étant communs à tous types de déploiement, le système doit donc permettre de mettre en place une structure hiérarchique afin de modéliser au mieux la structure organisationnelle, c'est-à-dire ***l'organisation*** et ***ses services***, les ***acteurs*** et les ***rôles*** qu'ils jouent dans l'organisation. Les annuaires électroniques ont donc naturellement été choisis.

Pour rappel, AdmiPRO est un système de gestion de flux administratifs *générique*. Le caractère générique du produit signifie que le système doit être convenablement paramétré avant d'être déployé. Par exemple, la réalisation au travers d'AdmiPRO de la procédure d'octroi des permis de bâtir amène à tenir compte d'éléments organisationnels propres à cette procédure :

- un permis de bâtir est déposé par un ***demandeur***
- les documents composants la demande ont été réalisés par un ***architecte***
- la ***commune*** et ***ses agents*** prennent en charge le dossier
- la ***DGATLP, la Direction Générale de l'Aménagement du Territoire, du Logement et du Patrimoine***, est un ministère du gouvernement wallon dont l'avis est parfois sollicité.

3.7.2 Choix techniques effectués

Il existe de nombreux systèmes d'annuaires, comme par exemple :

- IPlanet Directory Server de Sun-Netscape Alliance;
- Novell Directory de Novell;
- Oracle Internet Directory de Oracle;
- Active Directory de Microsoft;
- ...

Etant donné qu'AdmiPRO intègre plusieurs logiciels de la gamme Oracle, le choix s'est porté naturellement vers Oracle Internet Directory, version 2.1. Ce logiciel est compatible LDAP V.3 et garantit les besoins de la plate-forme administrative. Néanmoins, ce logiciel ne supporte pas les alias, ce qui a une répercussion sur le modèle d'adressage (cf. 3.7.3 Modélisation organisationnelle). Il est utile de noter que ce choix n'est pas seulement technique ou fonctionnel mais aussi financier.

L'accès à l'annuaire se fait via le protocole LDAP. Tout comme les modules AdmiPRO, les modules d'accès à l'annuaire électronique sont écrits en Java. Ils reposent sur les librairies JNDI et LDAP de Sun Microsystems.

3.7.3 Modélisation organisationnelle[28]

Le modèle des données AdmiPRO

Le modèle d'AdmiPRO est un modèle propriétaire mais qui hérite des objets standards de LDAP. De cette manière, il est facile de garder une compatibilité maximale tout en fournissant des services propres aux besoins de l'application.

Le point de départ de la réflexion est la modélisation de quatre objets de base[29] :

- l'organisation en tant que partenaire
- le service
- le rôle
- l'acteur ou personne physique (ppy)

Tous ces objets ont un correspondant dans le modèle des données de LDAP. La seule différence réside dans trois attributs :

- l'attribut mail (standard LDAP) est imposé à ces quatre objets
- l'attribut obligatoire AccessAdmiPro (indique si l'accès à AdmiPro est autorisé) et l'attribut optionnel URLPhoto (URL d'un fichier image) sont des attributs nouveaux et propres à un acteur

Le schéma LDAP est donc le suivant :

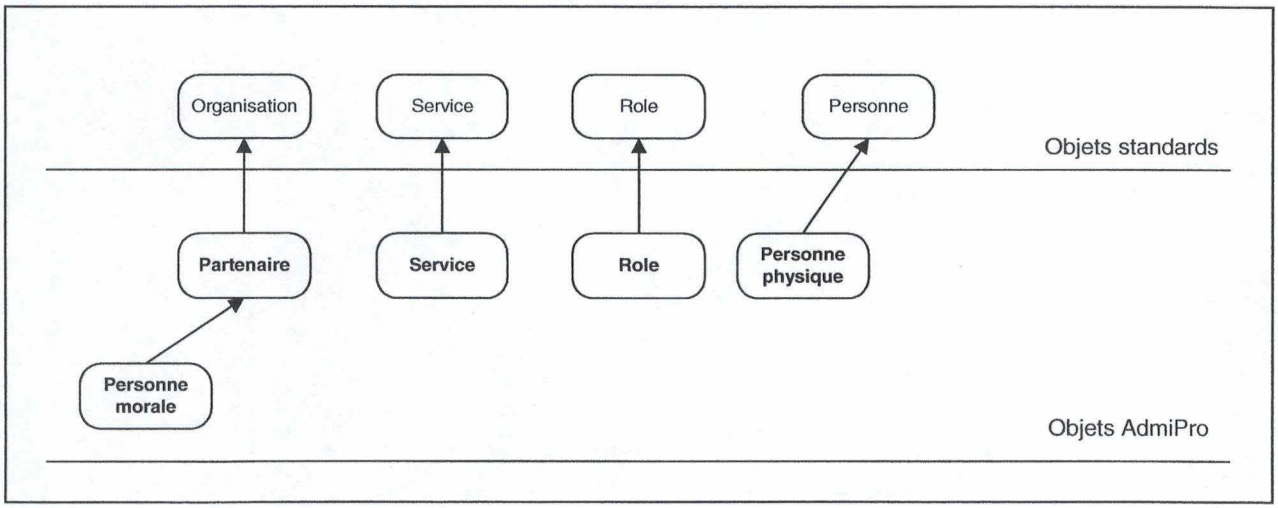

Figure 20. LDAP - MODELE DES DONNEES ADMIPRO

[28] Frankinet Ph., 2000.

[29] Les objets ont été définis dans un schéma entité-association repris dans Poos W., 2001. A titre indicatif, ce schéma est repris dans les annexes.

Les objets et attributs définis en format LDIF sont repris en annexe.

Le modèle d'adressage d'AdmiPro

Le modèle d'adressage est des plus courant, c'est-à-dire que les pays se trouvent au sommet de l'arbre, suivis par les organisations nationales et les régions, les provinces, ...

L'arbre permet ainsi de représenter les organisations, les services, sous-services et acteurs de manière naturelle. Par exemple, un acteur appartient à un service s'il est défini sous celui-ci. Dans le cas où un acteur doit être représenté dans plusieurs services, il est créé sous le service le plus important, les autres représentations sont en fait des rôles. Le fait que les alias ne sont pas utilisés provient de l'utilisation d'un annuaire ne supportant pas encore ce mécanisme.

Le cas des rôles est un peu plus particulier. Un rôle peut être joué par un ou plusieurs acteurs, parfois de services différents. Le modèle des données LDAP fournit une réponse simple à ce problème au travers de l'attribut "roleOccupant" de la classe "organizationalRole". Cet attribut multivalué contient les DNs des acteurs jouant ce rôle.

L'annuaire peut être distribué, les références ne sont pas à exclure. Elles seront planifiées selon l'environnement du client. Le suffixe par défaut a été fixé à "c=be".

Le modèle d'adressage mis en place dans AdmiPRO est le suivant :

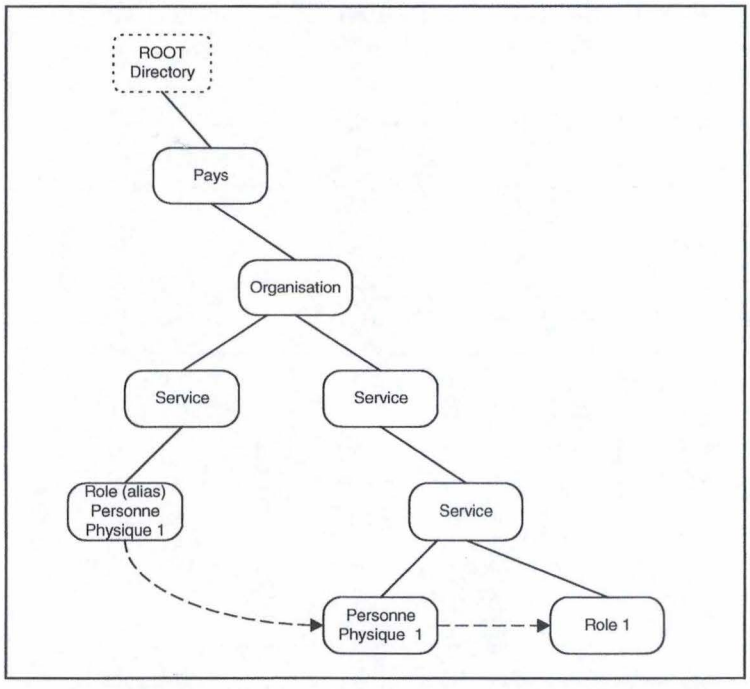

Figure 21. LDAP - MODELE D'ADRESSAGE ADMIPRO

et dont voici un exemple :

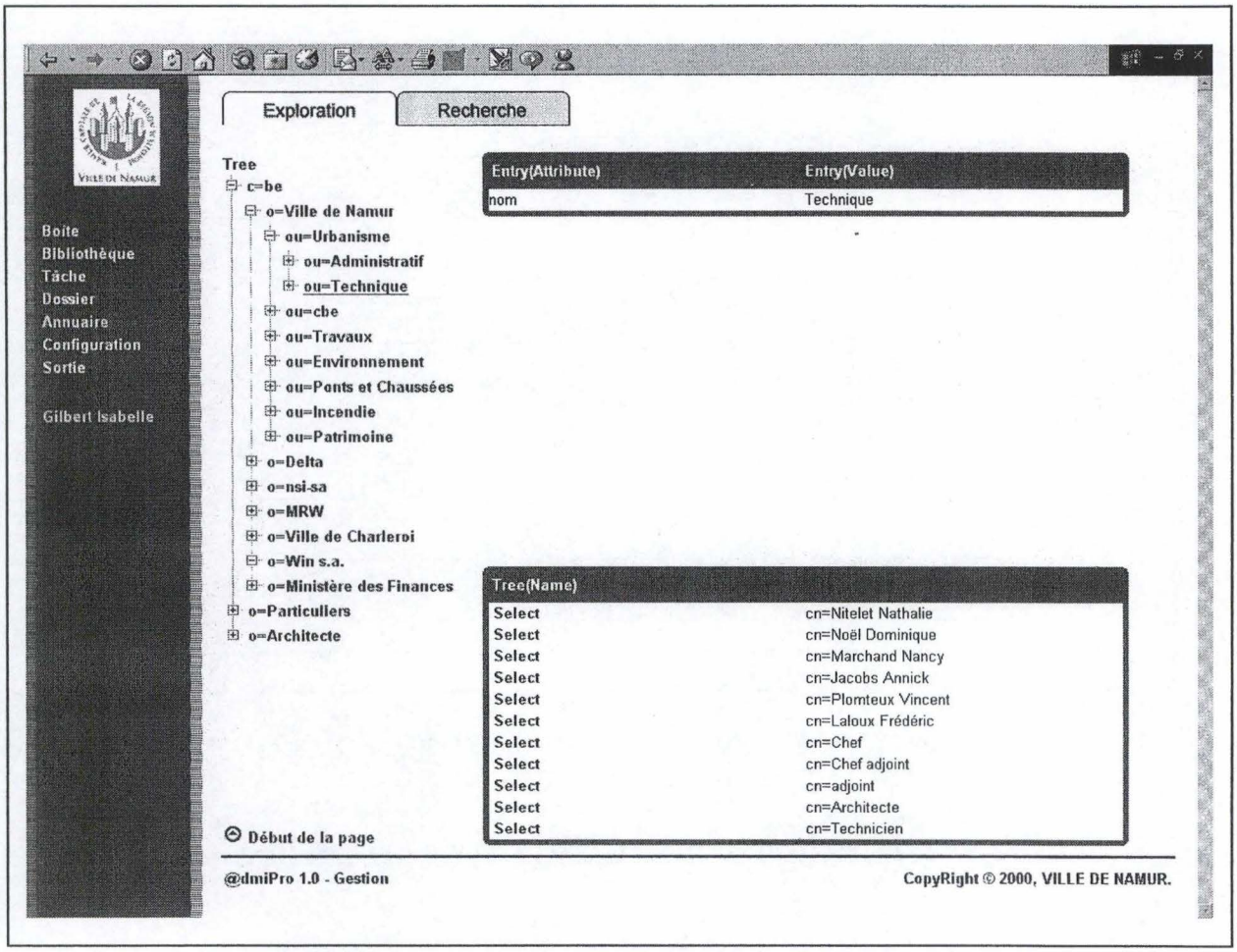

Figure 22. LDAP - ADMIPRO - ANNUAIRE ELECTRONIQUE

Le modèle des données AdmiPRO appliqué au cas PBFlow

Certains de ces objets sont liés directement avec le monde administratif, comme par exemple les communes, les ministères ou les provinces tandis que d'autres le sont à la procédure des demandes de permis de bâtir. Par exemple, l'architecte et le particulier sont toutes deux des personnes physiques, à différencier d'une personne morale agissant pour le compte d'une société.

La mise en place de la représentation organisationnelle liée à cette procédure nécessite l'introduction de nouveaux objets. Afin de respecter la définition de l'annuaire d'AdmiPRO, ces objets sont étendus à partir du modèle AdmiPRO.

La définition des objets est reprise des analyses fonctionnelles[30]. Le modèle des données AdmiPRO dans sa configuration PBFlow est le suivant[31] :

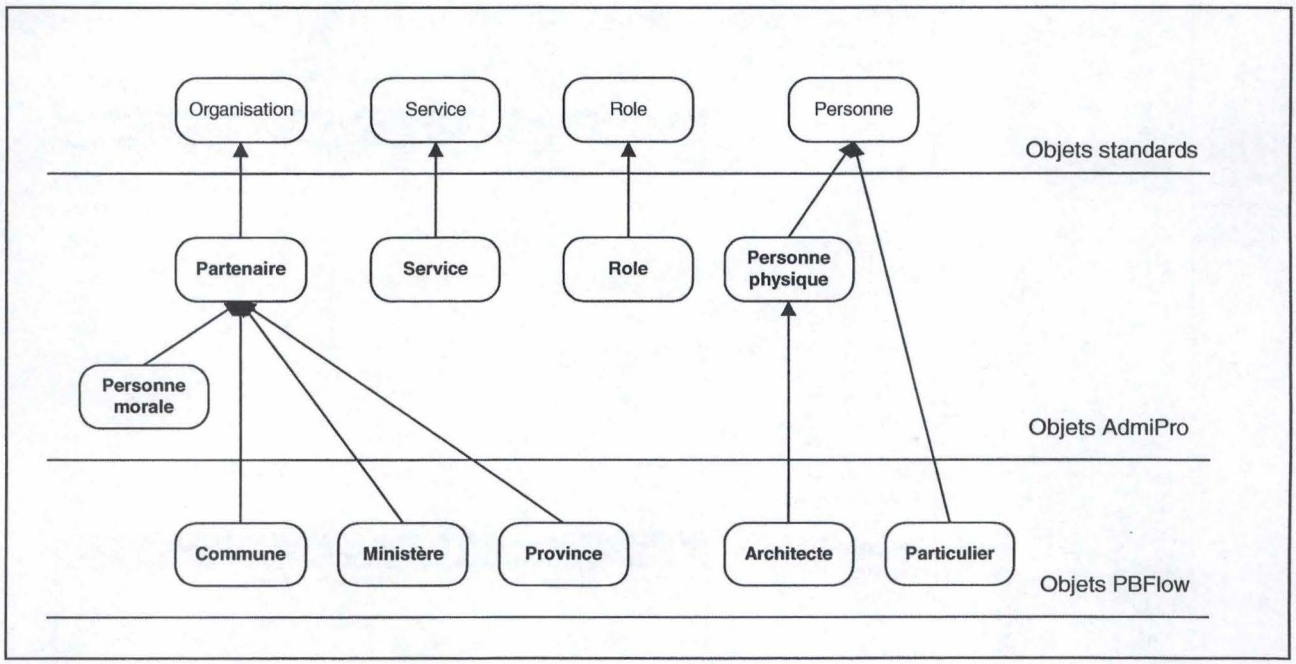

Figure 23. LDAP - MODELE DES DONNEES ADMIPRO APPLIQUE AU CAS PBFLOW

Le modèle d'adressage d'AdmiPRO appliqué au cas PBFlow

Le modèle d'adressage AdmiPRO dans sa configuration PBFlow est inchangé.

La sécurité et la politique d'accès

Actuellement, aucune authentification n'est requise pour accéder à l'annuaire d'AdmiPRO, toutes les lectures sont donc anonymes.

Par défaut, les implémentations actuelles des annuaires autorisent les mises à jours des entrées et du modèle des données à un groupe d'administrateurs prédéfinis. A charge donc de l'administrateur de l'annuaire de déterminer quelles personnes peuvent faire partie de ce groupe.

Une interface d'administration, qui ne sera pas décrite ici, permet de modifier le DIT et de l'adapter en fonction des besoins du client.

[30] Les objets ont été définis dans un schéma entité-association repris dans Poos W., 2001. A titre indicatif, ce schéma est repris dans les annexes.
[31] Frankinet Ph., 2001.

3.7.4 Réalisation technique[32]

Le logiciel AdmiPRO, écrit en Java, repose sur une librairie développée par NSI et appelée « JUnivers ». Elle fournit une série d'outils permettant de réaliser et de déployer rapidement une application Java. Un des avantages majeurs de cette couche logiciel est de fournir une manière unique d'accéder aux données, et ce quelle que soit la source d'information.

Par exemple, cette couche logicielle possède des connecteurs pour des sources d'informations telles que des bases de données ou des systèmes de messageries électroniques. L'utilisation de LDAP se fait donc en définissant un nouveau connecteur pour cette couche logicielle.

La solution apportée à AdmiPRO repose sur ce connecteur JUnivers. Il sert à transformer les demandes en requêtes compréhensibles pour LDAP et à retourner les données obtenues. Le connecteur doit satisfaire aux exigences suivantes imposées par la librairie JUnivers :

- fournir les classes définissant les types de requêtes disponibles
- fournir les classes de filtres booléens permettant de définir les critères de recherches pour chaque type de requête
- fournir les classes de connexions et d'exécution des requêtes

Le connecteur est détaillé dans les annexes (cf. A.7 AdmiPRO - Architecture Java du connecteur JUnivers).

Certaines applications Java chez NSI n'utilisent pas JUnivers. Afin de fournir un accès aisé aux annuaires électroniques pour ces applications, une seconde librairie a été créée. Cette dernière repose directement sur les modules développés par Sun Microsystems et propose une série de méthodes les plus couramment utilisées lors de l'interrogation d'un annuaire électronique, comme par exemple :

- les informations sur l'annuaire électronique
- la lecture et la manipulation du schéma de données
- les recherches et les listes
- les manipulations des entrées

Cette librairie est détaillée dans les annexes (cf. A.6 AdmiPRO - Architecture Java de la classe d'accès à LDAP).

[32] Frankinet Ph., 2001 (2).

L'architecture Java est la suivante :

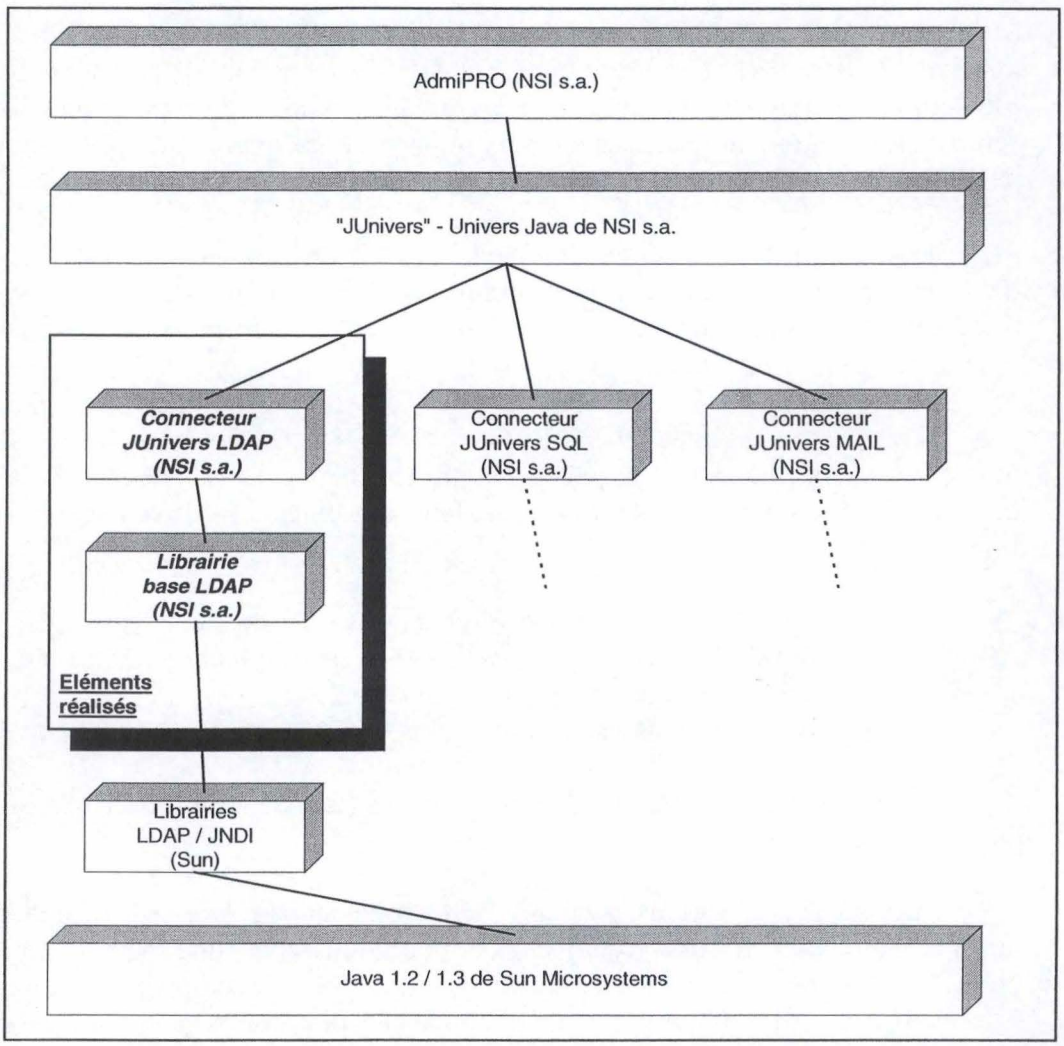

Figure 24. LDAP - ARCHITECTURE LOGICIELLE LDAP DANS ADMIPRO

Chapitre 4 Signature électronique et preuve

Ce chapitre aborde les problématiques de la preuve et de la signature électronique. Les aspects légaux, tant européens que belges, sont décrits. Les solutions techniques sont présentées et le choix fait dans AdmiPro est alors justifié.

4.1 Problématique de la signature électronique

Les réseaux ouverts, tel qu'Internet, sont en pleine expansion. Ils offrent des nouvelles possibilités économiques et permettent d'améliorer les services mis à disposition des clients, des citoyens et des entreprises.

Dans les transactions électroniques, comme dans de nombreuses procédures administratives, la partie prenante est amenée à signer divers documents et formulaires. Dès lors, comment va-t-elle s'y prendre pour signer ces documents destinés à être envoyés électroniquement ?

La mise en place d'un système où des transactions sont possibles met en lumière la problématique des signatures de documents électroniques, mais aussi il pose la question de l'authenticité de ce document et de l'identité véritable de l'expéditeur. Le problème n'est plus seulement technique, il est aussi légal.

Dès lors, il est nécessaire de répondre aux questions suivantes :

Le document est-il authentique ?
L'identité de l'expéditeur est-elle prouvée ?
Le document électronique est-il toujours une preuve recevable dans un tribunal ?
Les solutions techniques actuelles sont-elles suffisantes pour garantir l'authenticité du document et l'identité de l'expéditeur ?

Afin de tirer parti de ces nouvelles possibilités, il est nécessaire d'instaurer un cadre sûr en ce qui concerne l'authentification électronique. Les signatures électroniques permettent au destinataire de vérifier l'origine des données, c'est le principe de l'***authentification***, et de vérifier leur ***intégrité***. Afin d'être certain de l'identité de l'expéditeur, le destinataire doit avoir une preuve suffisante de son identité, notamment si une tierce partie de confiance confirme l'identité du correspondant. Ces deux principes, ***authentification et intégrité***, sont essentiels pour la mise en place de système transactionnel mettant en place les signatures électroniques.

Etant donné que les initiatives législatives se multiplient dans divers états européens, la communauté européenne a décidé de publier une directive visant à clarifier l'utilisation des signatures électroniques. Cette directive devra être transcrite dans les lois nationales.

Tous ces points sont développés au travers des lignes qui suivent. Après la synthèse de la directive européenne et des lois belges, quelques concepts liés à la cryptographie sont présentés au lecteur. La solution originale développée dans AdmiPRO est alors justifiée.

4.2Directive européenne[33]

4.2.1 Objectifs de la directive

La directive 1999/93/CE vise à assurer la reconnaissance des signatures électroniques en instituant un cadre juridique pour ces dernières. Elle établit un ensemble de critères servant de base à cette reconnaissance et clarifie l'utilisation de la signature dans les échanges commerciaux et administratifs.

4.2.2 Grands principes de la directive

Reconnaissance juridique

La signature électronique ne pourra être écartée pour la seule raison de sa forme électronique. La directive définit un ensemble de spécifications permettant de définir précisément le certificat, le prestataire de service et la signature utilisée, ce qui garantit que la signature aura même valeur qu'une signature manuscrite. Elle acquiert alors une force de preuve dans les procédures judiciaires.

Libre circulation

La libre circulation des biens et des services est garantit au sein de l'Union Européenne. Il en va de même des signatures électroniques. Elles sont seulement soumises à la législation et aux contrôles du pays d'origine, de même la prestation de service ne sera pas soumise à une autorisation obligatoire.

Responsabilité

Les fournisseurs de services se voient imposer certaines règles, en particulier sur la validité des informations contenues dans le certificat électronique.

Protection des données

La directive garantit que les prestataires de service et les organismes nationaux d'accréditation respectent les exigences relatives à la protection des données à caractère personnel. De plus, la directive garantit l'anonymat du consommateur en autorisant l'utilisation d'un pseudonyme en lieu et place du nom du signataire, et ce sans préjudice des effets juridiques liés à l'emploi de pseudonymes.

Neutralité technologique

La directive prévoit la reconnaissance de la signature électronique quelle que soit la technologie.

[33] Journal officiel des Communautés européennes, 1999

Aspects internationaux

La directive aborde aussi les mécanismes de coopération avec les pays tiers sur base de la reconnaissance mutuelle des certificats ou sur base de tout accord bilatéral ou multilatéral.

4.2.3 La signature électronique et le signataire

Avant de décrire ce qu'est une signature électronique, il est intéressant de voir comment la directive voit le signataire :

« le signataire est toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une entité ou personne physique ou morale qu'elle représente ».

Cette définition est très importante car elle ne fait **pas de distinction entre personne physique et personne morale**. Cela signifie qu'une personne morale peut signer un document électroniquement et ce dernier sera considéré comme un acte sous seing privé, au même titre qu'un écrit signé par une personne physique. Cela signifie également qu'il est possible à une personne morale de conclure des contrats par échanges de documents électroniques signés.

La directive aborde la signature électronique en donnant deux définitions :

1. Par signature électronique, on entend ***« une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données et qui sert de méthode d'authentification ».***
2. Par signature électronique avancée, on entend ***« une signature électronique qui satisfait aux exigences suivantes :***

   - ***être liée uniquement au signataire***
   - ***permettre d'identifier le signataire***
   - ***être créée par des moyens que le signataire puisse garder sous son contrôle exclusif***
   - ***être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable »***

Ces deux signatures électroniques sont complétées par la définition des certificats et certificats avancés, ce qui définit le moyen informatique utilisé lors de l'authentification et la signature électronique.

Par certificat, on entend ***« une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme son identité ».***

Par certificat qualifié, on entend ***« un certificat qui satisfait aux exigences visées à l'annexe I de cette même directive et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II de cette même directive ».***

L'annexe I reprend en fait les caractéristiques que doit avoir un certificat qualifié. Citons en autres :

- l'identité et la signature électronique avancée du prestataire de service
- le nom du signataire
- la durée de la validité de ce certificat
- les données liées à la création de la signature et correspondant aux données pour la création d'une signature par le signataire

4.2.4 Les prestataires de services de certification

Les prestataires de service de certification sont définis par la directive comme étant ***« toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques »***.

De plus, les prestataires sont soumis à des règles strictes, comme expliqué dans l'annexe II de la directive. Il y a d'une part la validité des données et d'autre part la sécurité du système.

La validité reprend, outre la durée de validité du certificat, un mécanisme sûr et immédiat de révocation d'un certificat émis. De plus, le prestataire a l'obligation de vérifier l'identité du signataire, et le cas échéant les qualités spécifiques de la personne.

Le prestataire doit disposer de moyens suffisants afin d'assurer le service, que ce soit des moyens financiers, informatiques ou humains.

4.2.5 Effets juridiques des signatures électroniques

La directive reconnaît qu'une signature électronique avancée a une valeur équivalente à la signature manuscrite et qu'elle est recevable comme preuve en justice. En fait la valeur juridique de la signature électronique contient deux clauses : l'une d'assimilation et l'autre de non-discrimination[34].

La clause d'assimilation consiste à assimiler la signature électronique à la signature manuscrite lorsque la signature électronique est dite avancée et repose sur un certificat qualifié émis par un dispositif sécurisé. Dans ce cas, la signature électronique est recevable comme preuve et bénéficie de la force probante accordée à la signature manuscrite.

La clause de non-discrimination s'applique lorsque les conditions liées à la clause d'assimilation ne sont pas remplies. La signature électronique ne peut être refusée au seul motif que la signature se présente sous forme électronique, qu'elle ne repose pas sur un certificat qualifié, qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité ou qu'elle n'a pas été créée par un dispositif sécurisé de création de signature. La signature électronique est donc recevable comme preuve, mais la personne invoquant cette signature électronique doit convaincre le juge de sa valeur probante.

[34] Antoine M., Gobert D., 2000

4.3Le droit belge

4.3.1 Les lois belges

La directive européenne 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 doit être transposer dans le droit belge. On peut mettre en avant les processus législatifs contribuant à cette reconnaissance :

- loi modifiant le Code civil relatif à la preuve qui introduit une définition fonctionnelle de la signature
- projet de loi sur la mise en place d'un régime juridique applicable aux prestataires de services de certification relatifs aux signatures digitales

4.3.2 Reconnaissance des preuves électroniques : loi du 20 octobre 2000

Jusqu'alors, les documents électroniques n'étaient pas recevables comme preuve devant un tribunal. En effet, conformément à l'article 1341 du Code civil[35] :

> *« Il doit être passé acte devant notaire ou sous signature privée, de toutes choses excédant une somme ou valeur de quinze mille francs, même pour des dépôts volontaires, et il n'est reçu aucune preuve par témoins contre et outre le contenu aux actes, ni sur ce qui serait allégué avoir été dit avant, lors ou depuis les actes, encore qu'il s'agisse d'une somme ou valeur moindre de quinze mille francs. Le tout sans préjudice de ce qui est prescrit dans les lois relatives au commerce ».*

Au-delà de la somme de 15 000 francs, il faut apporter une preuve écrite, par exemple sous seing privé. L'acte sous seing privé n'est pas clairement défini, même si l'article 1322 du Code civil apporte une réponse :

> *« L'acte sous seing privé, reconnu par celui auquel on l'oppose, ou légalement tenu pour reconnu, a, entre ceux qui l'ont souscrit et entre leurs héritiers et ayants cause, la même foi que l'acte authentique ».*

Ce texte n'étant pas assez précis, les juges ont décidé qu'un tel acte serait manuscrit, ce qui empêche tout document électronique de servir de preuve.

La loi du 20 octobre 2000 relatives aux règles de preuves a modifié le Code civil afin d'ajouter un alinéa à ce fameux article 1322 :

> ***« Peut satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte ».***[36]

[35] Wery E., 2000.
[36] Moniteur Belge, 22 Décembre 2000.

Grâce à cette loi, la signature ne doit plus nécessairement être écrite, ce qui implique que le juge ne peut refuser une signature électronique. Mais le juge reste libre d'apprécier la force probante d'une telle preuve, ce qui rend tout même son utilisation indécise.

Il y a néanmoins des restrictions[37] à la portée de cette loi :

- certaines dispositions du Code civil, du droit du travail, du droit administratif, ... ont des législations spécifiques nécessitant une signature manuscrite
- les actes authentiques sont exclus

4.3.3 Projet de loi sur les prestataires de services de certification[38]

Ce projet de loi apporte une réponse claire aux problèmes juridiques soulevés par l'emploi de signatures électroniques. Ce projet s'inspire de la directive européenne et en reprend les grands principes, c'est-à-dire[39] :

- délivrer des certificats qualifiés aux personnes physiques et morales, avec pour ces dernières, une limitation liée aux entités ayant une personnalité juridique.
- assurer une reconnaissance juridique de certaines signatures électroniques avancées produites par un dispositif sécurisé de création de signature et liées à un certificat qualifié.
- adopter un cadre neutre d'un point de vue technologique
- définir un système libre d'accréditation pour les prestataires de services de certification.

Cette loi reprend les diverses définitions de la directive européenne dans son article 2 mais le point essentiel de cette loi est certainement l'article 4, § 4 :

« § 4. Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur base d'un certificat qualifié et créée par un dispositif sécurisé de création de signature satisfait aux exigences de l'article 1322, alinéa 2 du Code civil, que cette signature soit réalisée par une personne physique ou morale ».

La portée juridique de la signature électronique avancée est importante, car si cette signature électronique avancée est créée par un dispositif sécurisé et combinée à un certificat qualifié, elle a force probante. Elle a donc les mêmes effets que la signature manuscrite et le contrôle préalable du juge n'est plus nécessaire[40].

Le reste du projet de loi traite des prestataires de services, de leurs missions et obligations.

---

[37] Struyven D., 2001.
[38] Chambre des représentants de Belgique, 2001.
[39] Gobert D., 2000.
[40] Struyven D., 2001

4.3.4 Effets juridiques de la loi et du projet de loi

La transposition complète des clauses d'assimilation et de non-discrimination de la signature électronique prévue par la directive européenne n'est possible que par la combinaison du nouvel alinéa ajouté à l'article 1322 du Code civil et par l'article 4 § 4 du projet de loi fixant les règles relatives au cadre juridique pour les signatures électroniques.

La modification du code civil introduit une nouvelle approche de la signature et admet la recevabilité d'une signature électronique mais en laissant au juge l'appréciation qu'il accorde à cette signature (clause de non-discrimination). Enfin, le projet de loi va plus loin en accordant force probante aux signatures électroniques avancées telles que définies par la directive européenne : ces signatures bénéficient des mêmes effets juridiques qu'une signature manuscrite (clause d'assimilation)[41].

4.3.5 Les manquements de la loi

Il est évident que nous ne sommes pas tous égaux devant la nouvelle société de l'information pour des raisons financières ou d'éducation. Or chaque citoyen ayant droit à un traitement équitable, la signature manuscrite est et sera toujours utilisée.

La loi et le projet de loi reconnaissent la légalité de la signature électronique. Cela signifie que le client ou citoyen utilise des moyens informatiques pour correspondre avec des sociétés privées ou l'administration, elles-mêmes utilisant des moyens informatiques pour traiter ces demandes.

Les systèmes dits "papier" et ceux dits "électronique" doivent coexister et garantir à tous une reconnaissance équivalente. On peut donc se poser légitiment la question suivante :

comment passer d'un système à l'autre tout en garantissant une valeur légale aux transactions et aux documents ?

Les deux cas ci-dessous sont représentatifs de cette situation :

- *l'utilisation d'une copie papier d'un document signé électroniquement*
- *l'utilisation électronique d'un document possédant une signature manuscrite*

Malheureusement, la loi actuelle laisse planer certaines incertitudes, donc une insécurité juridique.

[41] Wery E., 2001

4.4Notion de cryptographie[42]

Afin de bien comprendre les mécanismes mis en place dans la signature électronique, il est utile d'avoir quelques notions de cryptographie. Ces notions portent sur les deux cryptosystèmes que sont les systèmes à clés secrètes et les systèmes à clés publiques.

4.4.1 Cryptographie à clé secrète

La cryptographie à clé secrète, ou cryptographie symétrique, repose sur le partage d'une et une seule clé. Ainsi, la clé est utilisée par l'expéditeur pour chiffré un contenu et par le destinataire pour le déchiffrement tel que le représente la figure ci-dessous :

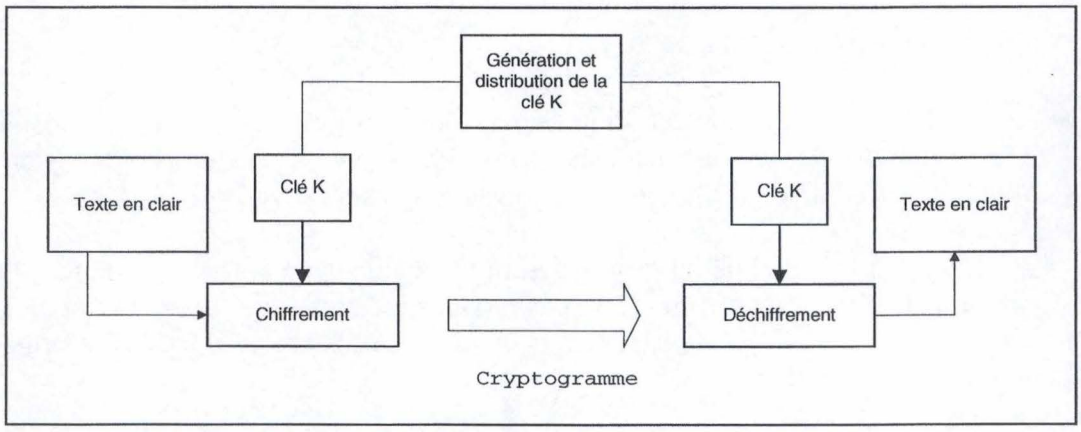

Figure 25. SIGNATURE - CHIFFREMENT AVEC CLE SECRETE

L'authentification des acteurs se fait en utilisant le mécanisme de "challenge-response". L'expéditeur choisi un nombre aléatoire qu'il chiffre et envoie au destinataire. Ce dernier répond en émettant la réponse chiffrée avec la clé partagée.

L'authentification de document se fait en calculant un résumé à partir du contenu à échanger. Ce résumé est chiffré et expédié avec le document. Le destinataire doit pouvoir recalculer ce résumé et le comparer à celui qui a été reçu.

[42] Ramaekers J.

4.4.2 Cryptographie à clé publique

La cryptographie à clé publique, ou cryptographie asymétrique, ne partage aucune clé. Chaque interlocuteur possède un couple de clé, la clé privée et la clé publique.

Le chiffrement d'un contenu se fait en utilisant la clé publique du destinataire. Lui seul pourra alors déchiffrer le message avec sa clé privée.

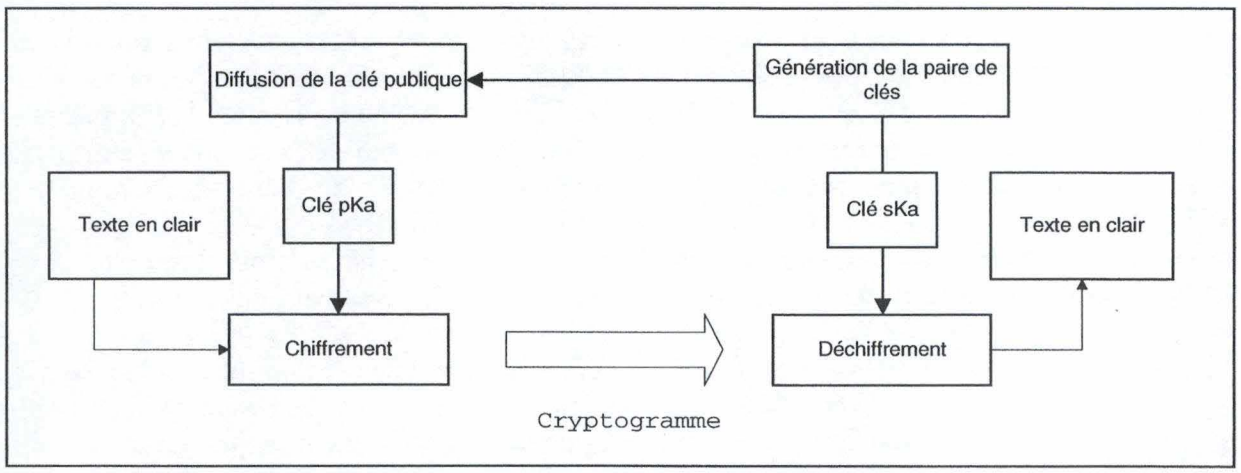

Figure 26. SIGNATURE - CHIFFREMENT AVEC CLE PUBLIQUE

L'authentification des acteurs se fait en signant un challenge avec la clé privée. Le destinataire pourra vérifier la validité du challenge en utilisant la clé publique de l'émetteur.

L'authentification de document utilise les mêmes mécanismes que les cryptosystèmes symétriques, c'est-à-dire qu'un résumé est calculé à partir du document. Ce résumé est signé à l'aide de la clé privée de l'émetteur. Ce mécanisme garantit non seulement le contenu du message mais aussi l'identité de l'expéditeur.

4.5Solution pour la signature électronique : le système PKI

Un système PKI (*Public Key Infrastructure*) est un ***système à clé publique***. L'élément central est l'autorité de certification produisant des certificats électroniques au format X509.

4.5.1 Autorité de certification

L'autorité de certification, ou *Certificate Authority (CA)* en anglais, produit les certificats électroniques au format X509. Elle est responsable du stockage, de la distribution des clés et de la révocation des certificats. Chaque système PKI possède généralement un ***annuaire électronique*** reprenant l'ensemble des certificats émis par le système. Cet annuaire est consultable par le public.

La plupart des autorités actuelle de certification génèrent trois classes de certificats, chaque classe correspondant à un niveau de certification :

- la classe 1 est purement démonstrative. La seule garantie réside dans le fait que le certificat généré est bien lié à une adresse de courrier électronique valable. L'identité du propriétaire de cette boîte n'est pas garantie.

- la classe 2 est délivré sur présentation de papiers d'identité. L'identité du propriétaire du certificat peut ainsi être vérifiée.

- la classe 3 est la plus sûre car le futur propriétaire du certificat doit se présenter physiquement à un bureau d'enregistrement afin de valider son identité.

L'autorité de certification d'un système PKI respecte bien les contraintes légales imposées à toute autorité de certification voulant mettre en place la distribution de certificats qualifiés comme cela est définit dans la directive européenne et les lois belges[43].

[43] Chambre des représentants de Belgique, 2001 et Journal officiel des Communautés européennes, 1999, Annexe II.

4.5.2 Certificat X509

PKCS (*Public Key Cryptography Standard*) est un standard utilisé dans la cryptographie à clé publique, définissant entre autres les formats des certificats électroniques.

Le format actuel le plus connu est le format X509 version 3 représenté par la figure suivante :

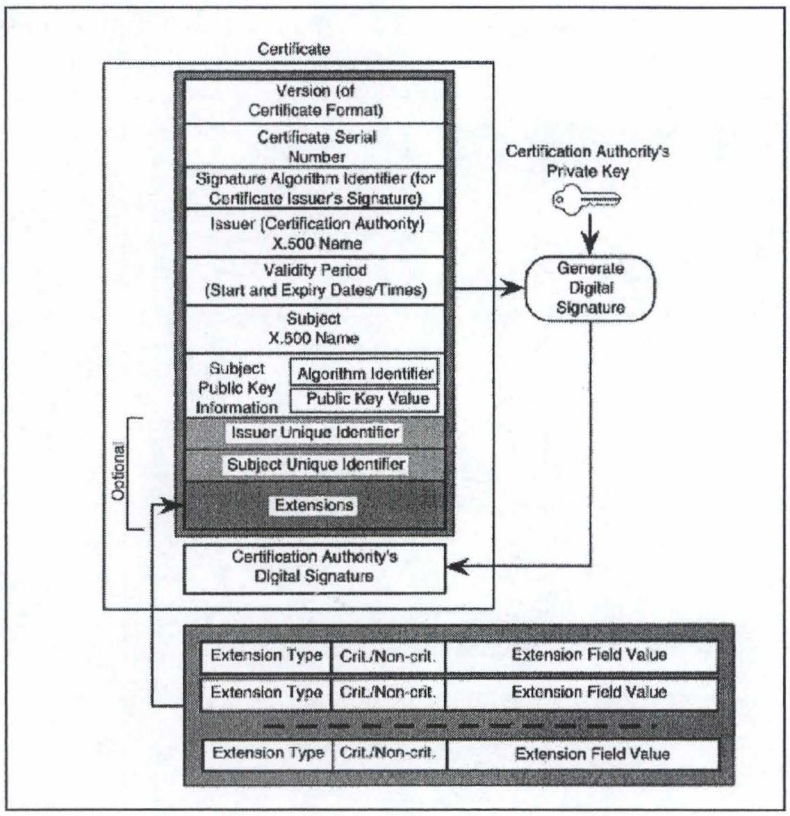

Figure 27. SIGNATURE - FORMAT DES CERTIFICATS X509 V.3

Le certificat a les propriétés suivantes :

- *version :* Version du certificat
- *serial number :* Identifiant unique pour le certificat, assigné par la CA qui a distribué le certificat
- *signature :* Identifiant de l'algorithme de la signature utilisé par la CA pour signer le certificat
- *issuer :* Le nom au format X.500 de la CA qui a distribué le certificat
- *validity period :* Période de validité du certificat (Date et heure de début et de fin du certificat)
- *subject :* Le nom au format X.500 du propriétaire de la clé privée, dont la clé publique correspondante est certifiée

- *subject public-key information :* La valeur de la clé publique pour le sujet et l'identifiant de l'algorithme avec lequel cette clé publique doit être utilisée
- *issuer unique identifier :* Une chaîne de caractères optionnelle utilisée pour rendre le nom de la CA non-ambigu dans le cas où le même nom aurait été réassigné à différentes entités
- *subject unique identifier :* Une chaîne de caractères optionnelle utilisée pour rendre le nom du sujet non-ambigu dans le cas où le même nom aurait été réassigné à différentes entités
- *extensions :* Utilisé pour les extensions futures

La plupart des navigateurs Internet utilisent ce type de certificat. Les propriétés de ces derniers peuvent facilement être consultées, comme le témoigne la figure ci-dessous :

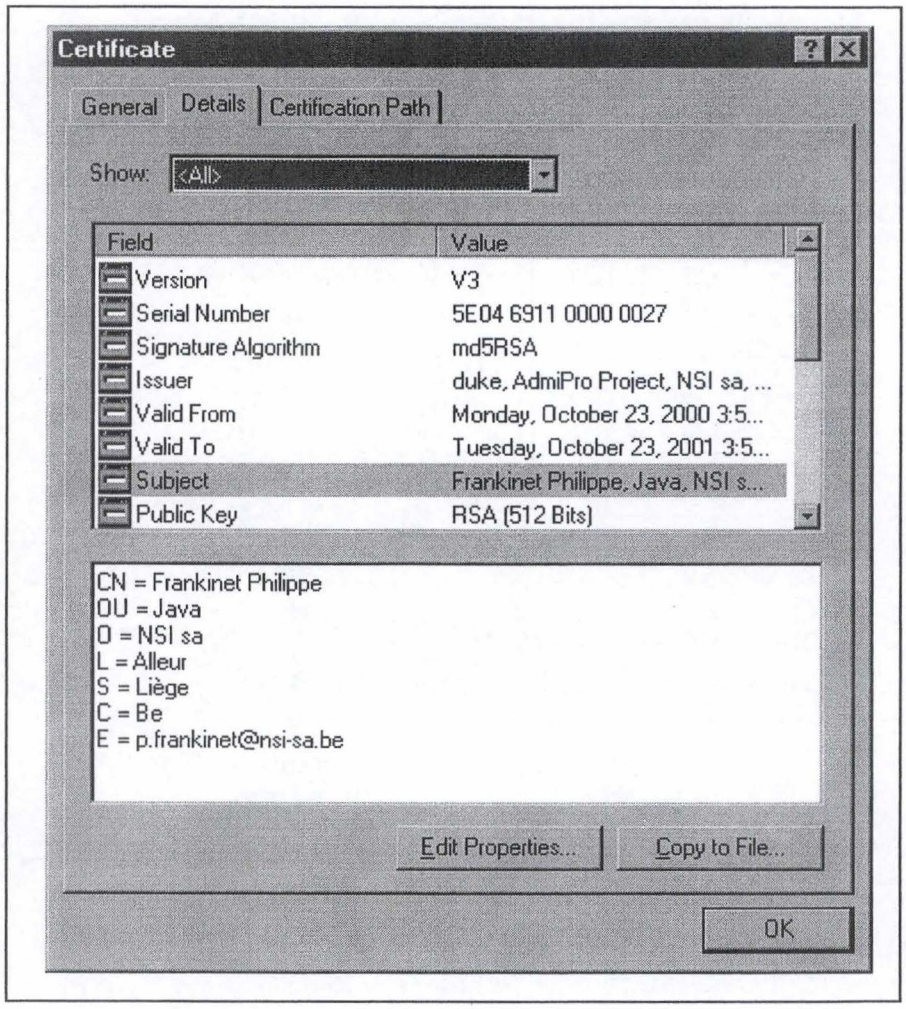

Figure 28. SIGNATURE - CERTIFICAT REPRIS PAR UN NAVIGATEUR INTERNET

4.6 La signature électronique dans AdmiPRO[44]

La signature électronique dans le logiciel AdmiPRO est le résultat d'une veille technologique sur les techniques de signature. L'implémentation originale mise en place suit le processus suivant :

- étude des besoins
- choix technique
- conformité aux lois
- réalisation technique

La mise en place de la signature électronique dans AdmiPRO reprend les mêmes fonctionnalités que celles développées dans le cadre du projet PBFlow[45]. Les besoins d'AdmiPRO sont donc semblables à ceux de PBFlow.

Le choix technique doit se porter sur une solution qui garantit le respect des lois sur l'utilisation de la signature électronique. Ce choix doit aussi être compatible avec les choix déjà effectués dans AdmiPRO.

Enfin, la réalisation technique décrit l'architecture logicielle mise en place. Pour des raisons de confidentialité, le code développé ne fait pas partie de ce document.

4.6.1 Besoins d'AdmiPRO en matière de signature électronique

AdmiPRO a essentiellement deux types de besoins en matière de signature électronique, à savoir un besoin fonctionnel et un besoin lié à la technologie.

La signature électronique d'un document est bien entendu le besoin fonctionnel de base pour tout système transactionnel permettant l'échange de document. Néanmoins, certains documents nécessitent plusieurs signatures, alors appelées signatures parallèles ou de même niveau.

Le besoin technologique est lié à l'implémentation des modules AdmiPRO, et plus particulièrement au fait que le client ne dispose que d'un navigateur Internet standard comme support de l'interface homme-machine.

[44] Frankinet Ph., 2001 (3).
[45] Ramaekers B., 2000 et Michot O., 2000.

4.6.2 Technologie choisie

NSI s.a. et WIN s.a. ont choisi Belgacom E-Trust comme partenaire dans la mise en place de la signature électronique. Il est bien entendu évident que ce partenaire n'est nullement imposé, mais il est un prestataire de service de certification respectant les critères de la directive.

Afin de rester cohérent avec le logiciel AdmiPRO écrit en Java, les modules de signatures et de vérifications sont basés sur une librairie Java fournie par cette société. Le fait que la librairie soit écrite dans ce langage permet également au module de signature de s'exécuter sur le navigateur Internet du client. Il s'agit d'une différence marquante, bien que sans conséquences, avec le logiciel PBFlow basé sur les technologies Microsoft.

A l'heure actuelle, le seul support mis à disposition des signataires pour les certificats qualifiés est le lecteur de disquette. Bien que cela puisse paraître une limitation, il n'en est pourtant rien. En effet, dans un système à grande échelle mettant en relations des citoyens et l'administration, il n'est pas certain que ceux-ci disposent de systèmes sophistiqués tels que les smart cards.

4.6.3 Conformité à la directive et aux lois belges

La signature électronique mise en place dans AdmiPRO repose sur un certificat électronique X509, c'est-à-dire un certificat qualifié émis par un prestataire de certification qualifié comme l'entend la directive européenne.

4.6.4 Réalisation technique

Dans AdmiPRO, les documents utilisés et produits lors du processus sont stockés dans un système propriétaire de gestion électronique de dossiers, c'est-à-dire dans une base de données relationnelles. Afin de faciliter la manipulation des documents, il a été décidé de stocker, non pas le document associé à sa signature, mais bien la signature elle-même[46]. Cela garantit une occupation minimale de l'espace de stockage en cas de multiples signatures d'un même document.

Avec une telle solution, il est évident qu'un document signé ne peut être modifié, de même qu'il ne sera pas proposé plusieurs versions d'un même document pour signature.

[46] Le schéma entité-association lié au modèle des documents se trouve en annexe.

Mécanisme de signature mis en place

Le mécanisme de signature mis en place est donc le suivant :

1. Le signataire a la possibilité de visualiser, supprimer ou signer un document qu'il a introduit dans le système, comme le représentent la figure ci-dessous :

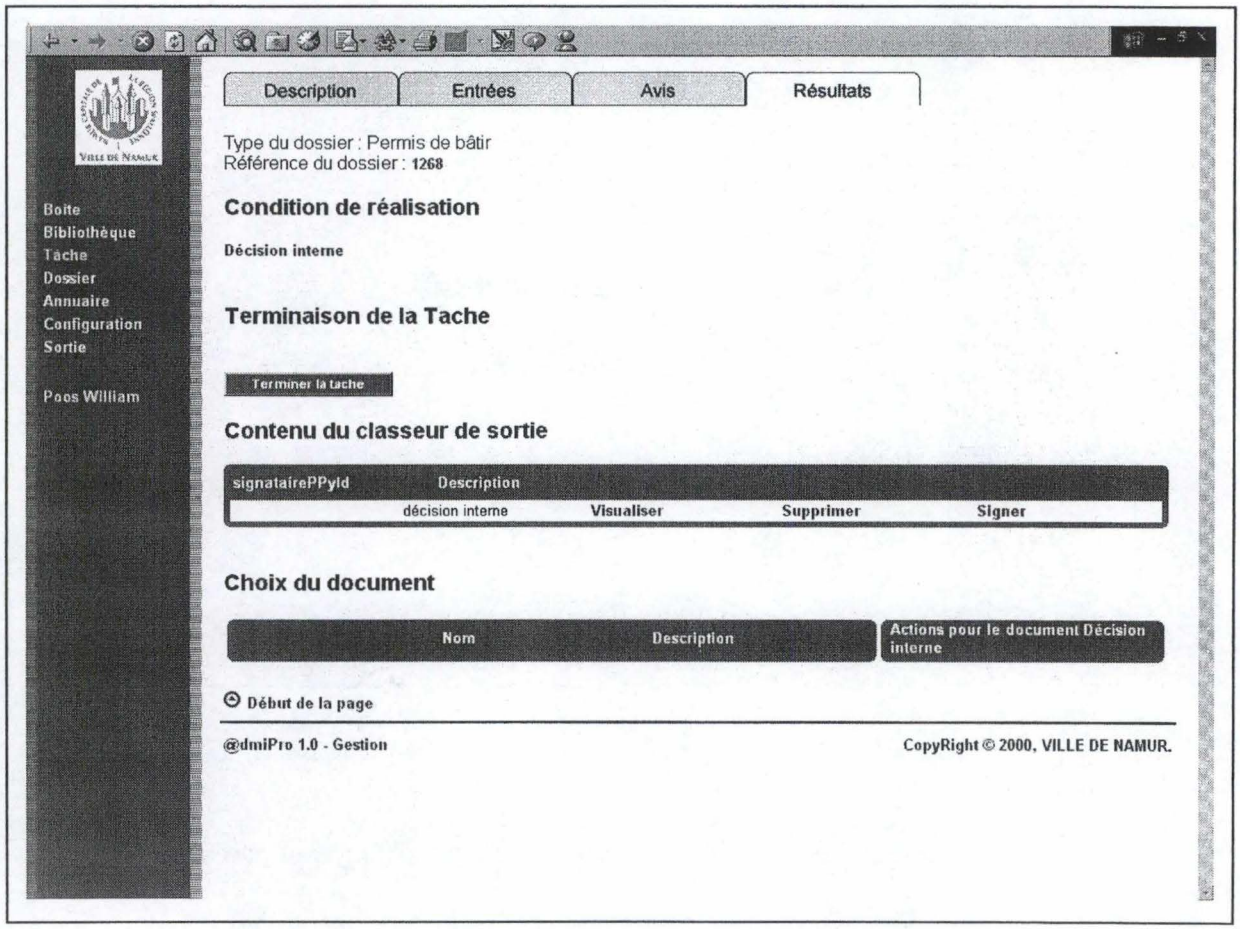

Figure 29. SIGNATURE - DOCUMENT D'UN CLASSEUR DE SORTIE PROPOSE POUR SIGNATURE

2. Afin de procéder à la signature, le signataire doit encoder la passphrase permettant de lire sa clé privée utilisée pour la signature.

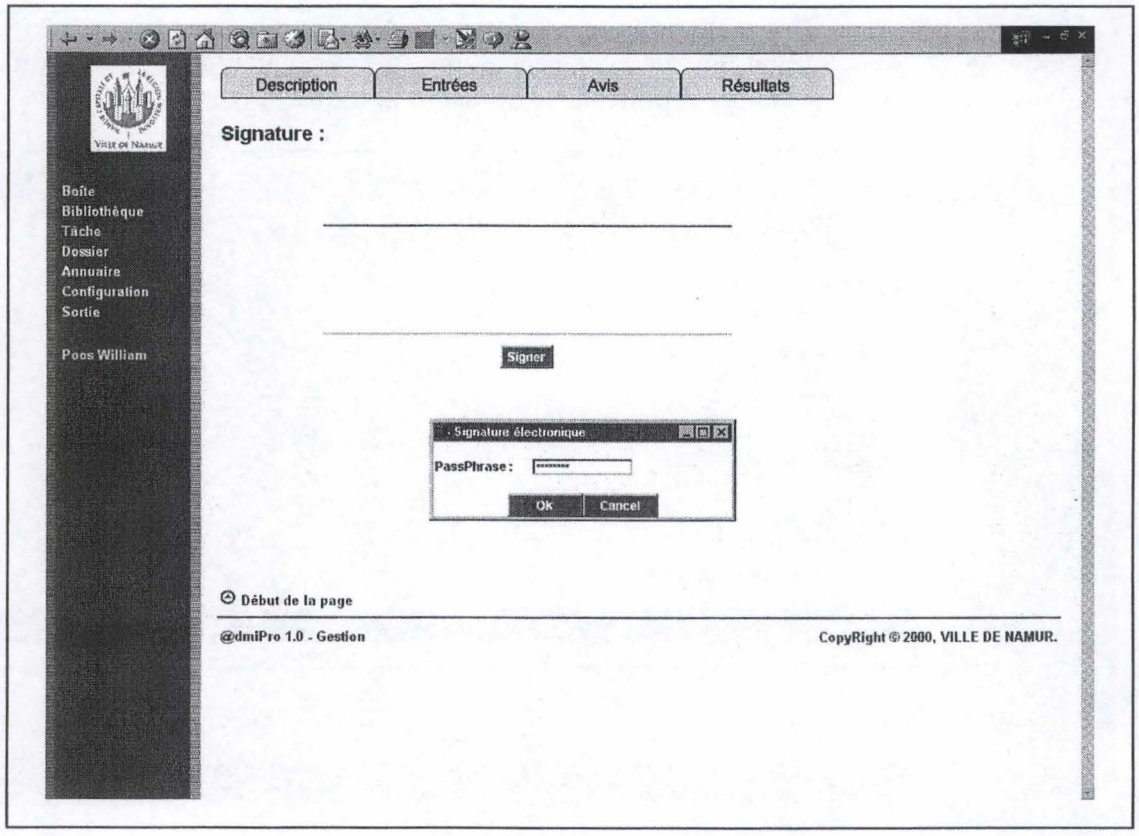

Figure 30. SIGNATURE - ENCODAGE DE LA PASSPHRASE

3. Une fois la passphrase vérifiée, le document est téléchargé pour signature.

4. La signature ainsi produite est expédiée au système afin d'être validée.

5. Le module de vérification s'assure que la signature reçue correspond bien au document qui se trouve dans la gestion électronique des dossiers et que le certificat du signataire est bien valide.

6. La signature est insérée dans la gestion électronique des dossiers.

7. Le client est notifié du succès de l'opération.

La figure ci-dessous représente le déroulement de l'opération de signature :

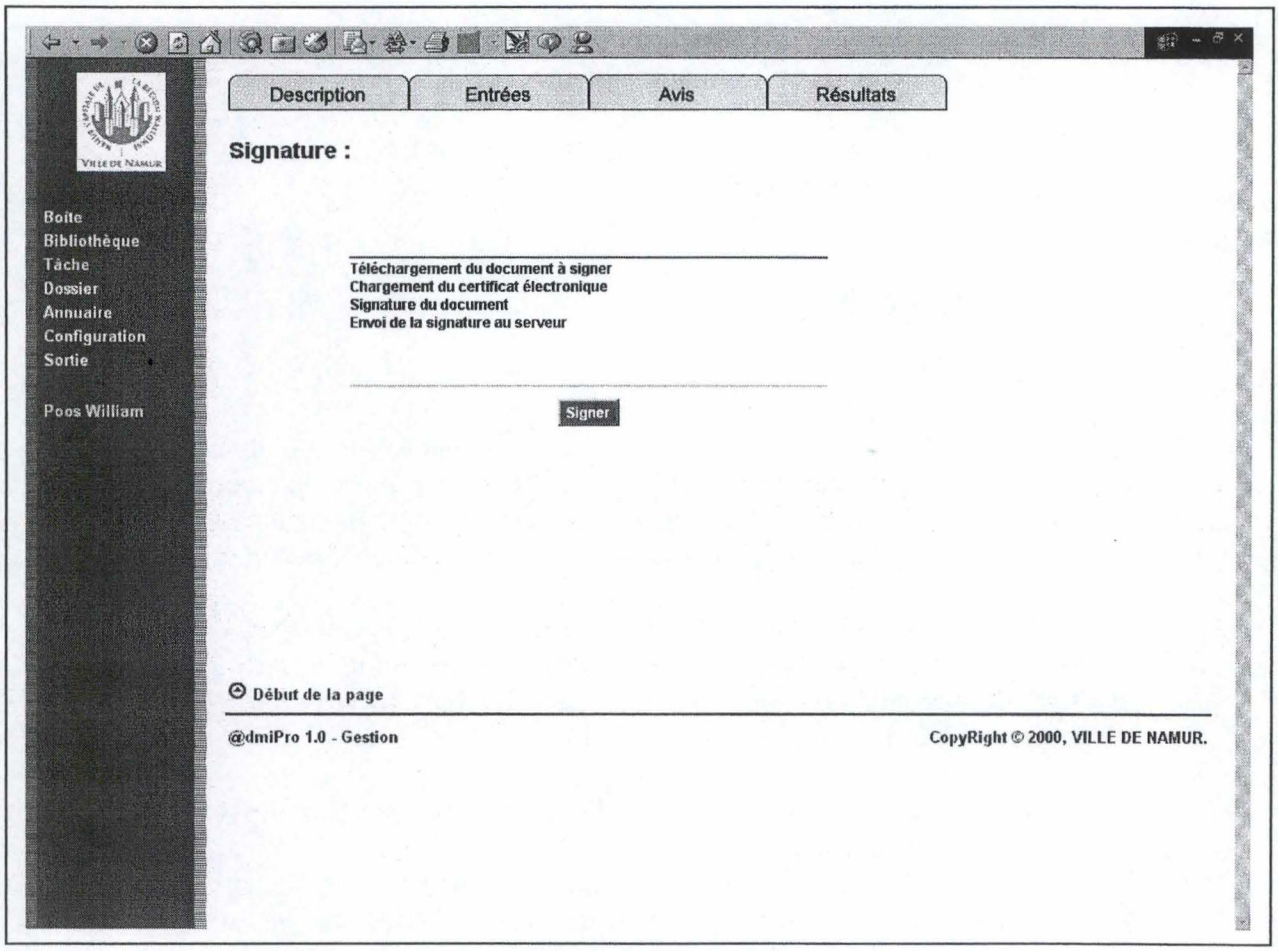

Figure 31. SIGNATURE - OPERATION DE SIGNATURE

Il est utile de remarquer que la directive européenne a introduit des recommandations[47] afin de vérifier la signature de façon sécurisée, à savoir que :

- les données utilisées pour vérifier la signature correspondent aux données affichées à l'intention du vérificateur;
- la signature soit vérifiée de manière sûre et que le résultat de cette vérification soit correctement affiché;
- le vérificateur puisse, si nécessaire, déterminer de manière sûre le contenu des données signées;
- l'authenticité et la validité du certificat requis lors de la vérification de la signature soient vérifiées de manières sûre;

[47] Journal officiel des Communautés européennes, Annexe IV, 1999.

- le résultat de la vérification ainsi que l'identité du signataire soient correctement affichés;
- l'utilisation d'un pseudonyme soit clairement indiqué;
- tout changement ayant une influence sur la sécurité puisse être détecté.

Ces recommandations sont suivies dans AdmiPRO, même si le vérificateur est un module du système d'information.

Architecture Java

Deux éléments sont à prendre en considération, à savoir :

- le logiciel AdmiPRO, écrit en Java, repose sur une librairie développée par NSI et appelée « JUnivers ». Elle fournit une série d'outils permettant de réaliser et de déployer rapidement une application Java.
- le client ne dispose que d'un navigateur Internet standard

La signature électronique proprement dite sera réalisée au travers d'un applet Java. Cette solution permet de disposer des librairies du prestataire de certification (Belgacom E-Trust) et est compatible avec tout navigateur Internet. La seule restriction vient de la machine virtuelle Java limité dans sa version 1.1

L'applet est Java est décrite dans les annexes (cf. A.8 AdmiPRO - Architecture Java de l'applet de signature).

La vérification de la signature électronique est effectuée par un servlet. Ce module repose sur la librairie JUnivers et utilise les librairies de signatures électroniques du prestataire (Belgacom E-Trust).

Le module de vérification est décrit dans les annexes. (cf. A.9 AdmiPRO - Architecture Java du module de vérification des signatures).

Le schéma suivant décrit l'architecture Java mise en place :

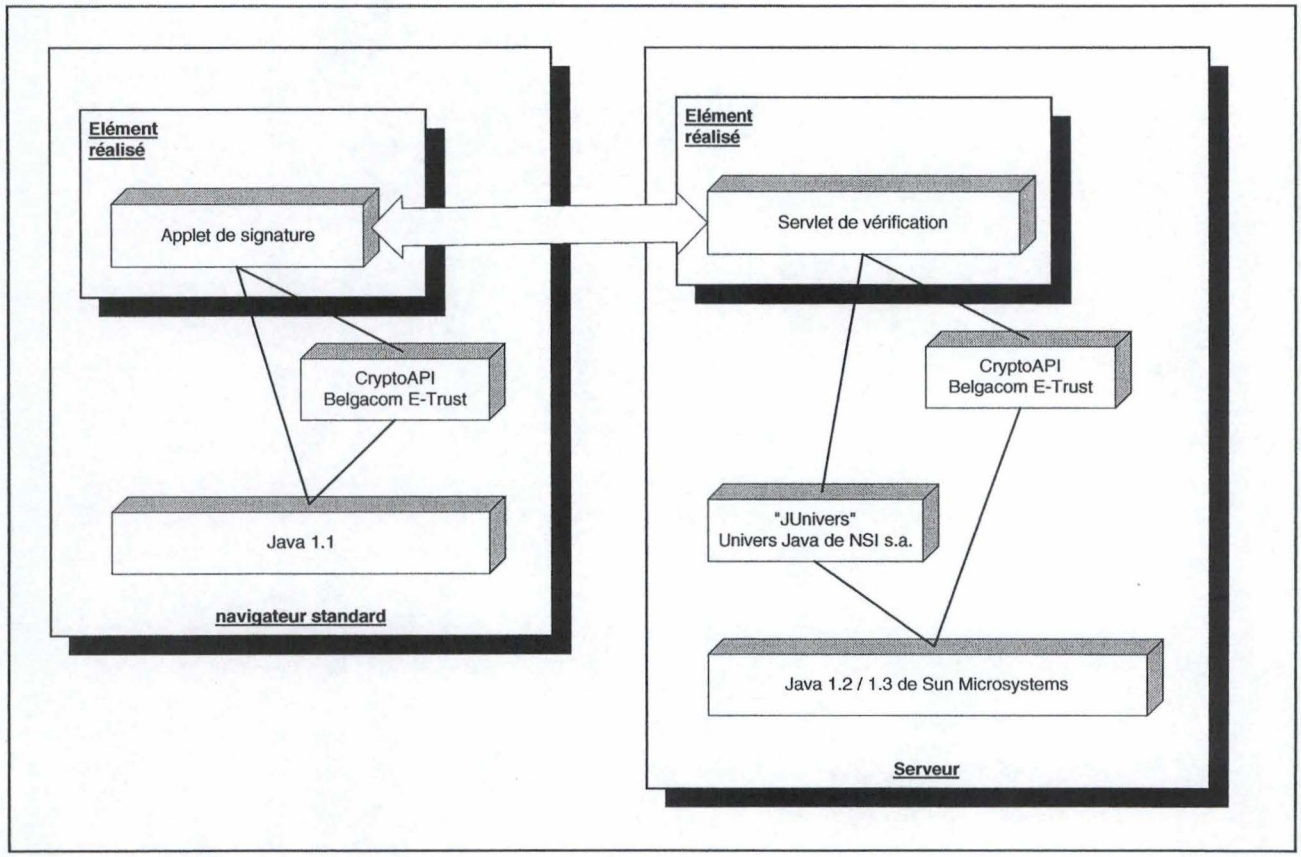

Figure 32. SIGNATURE - ARCHITECTURE JAVA DE LA SIGNATURE ELECTRONIQUE DANS ADMIPRO

CONCLUSION

Dans ce travail, nous avons abordé le concept du guichet unique et son application au travers d'un cas pratique. Nous avons étudié deux facteurs influençant la mise en place d'une telle solution, à savoir les problèmes de représentation organisationnelle et les problèmes liés à l'utilisation de la signature digitale dans les transactions électroniques.

La mise en évidence des problèmes rencontrés lors des réformes administratives a mis en lumière la nécessité d'adapter le mode de prestation des services administratifs. Le guichet unique est une des solutions envisagées afin d'améliorer ces prestations; et la définition et la classification de ces guichets ont permis de mieux cerner l'utilisation d'une telle solution.

L'illustration de ce concept au travers d'un cas pratique a servi de base à la réflexion portant sur les difficultés rencontrées à la mise en place du guichet unique. Dans ce travail, nous nous sommes attachés aux problèmes de représentation organisationnelle et de signature électronique. Outre une synthèse des concepts rencontrés, des solutions originales et personnelles ont été apportées à un des premiers guichets uniques « True One Shop » mis en place en Belgique.

La représentation organisationnelle fait partie d'un des quatre facteurs influençant la mise en place du guichet. Ce problème peut être résolu par l'utilisation des annuaires électroniques et du protocole LDAP. Les informations de ces systèmes sont organisées de manière hiérarchique, ce qui convient parfaitement à la représentation de la structure d'une organisation.

Le deuxième facteur étudié concernait le cadre légal, et plus particulièrement la signature dans les transactions électroniques. L'étude des textes légaux, tant européens que belges, a démontré que la législation permet, ou permettra très bientôt, de mettre en place des systèmes transactionnels faisant appel à la signature électronique de documents. La technologie nécessaire pour la signature électronique est déjà disponible grâce aux systèmes PKI qui permettent de délivrer des certificats électroniques certifiés par des tiers (de confiance).

Les perspectives des guichets uniques sont nombreuses, mais trois initiatives mériteront une attention particulière dans un futur proche : la phase II du logiciel AdmiPRO, l'utilisation par le citoyen belge d'une carte d'identité électronique et l'utilisation du *Legal XML* dans l'échange de documents avec les autorités judiciaires.

Voici, en quelques mots, la description de ces trois initiatives :

- La phase II d'AdmiPRO, en cours actuellement, doit permettre l'intégration des processus inter-organisationnels, entre autres via la mise en place d'une plate-forme B2B (Business to Business). Elle doit permettre aussi le déclenchement de tâche d'un processus d'une autre organisation et favoriser l'échange des dossiers administratifs.

Cette phase II a fait l'objet d'un mémoire de fin d'étude dont voici les références :

ADMIPRO PHASE 2
Gestion de suivi des dossiers de permis de bâtir
Didier Husson
Travail de fin d'études
Année académique 2000-2001
H.E.M.E.S.
I.E.S.S.L.

- La carte d'identité électronique est une initiative du gouvernement fédéral belge[48]. Cette initiative, prise en l'an 2000, porte sur la mise à disposition d'une carte d'identité électronique pour le citoyen belge. Elle doit permettre l'échange électronique de données entre les différentes autorités et leurs clients, à savoir les citoyens et les entreprises.

  La proposition de travail du gouvernement porte sur l'intégration des données d'identité et les données liées aux soins de santé. Les récentes modifications du code civil permettent de mettre en service cette carte d'identité électronique dont les fonctions seraient les suivantes :

  - identificaton
  - authentification
  - preuve de la qualité de la personne (mandat, fonction, ...)
  - porteuses de programmes
  - porteuses de données électroniques

  La carte sera délivrée par une autorité d'enregistrement. L'autorité de certification a pour rôle la création du certificat électronique. La carte serait finalement délivrée au citoyen sous la forme d'une carte à puce protégée par un code. Le phase pilote de ce projet a débutée en 2001 et implique plusieurs villes en Belgique.

- Legal XML est un standard non-propriétaire permettant de définir des documents électroniques utilisés par le monde judiciaire[49]. Il s'agit de définir des marqueurs supplémentaires utilisés dans un document XML. Ce langage est promu par Legal XML (www.legalxml.org).

Enfin, ce travail peut être complété par l'étude des deux autres facteurs influençant la mise en place d'un guichet unique, à savoir le facteur lié aux technologies utilisées et l'impact économique d'une telle solution. Il serait aussi utile de voir quelle sera la réponse du législateur ou des juges faces aux manquements de la reconnaissance et de l'utilisation de la signature électronique.

[48] Robben F., 2001.
[49] Georgia State Research Foundation, 2000

BIBLIOGRAPHIE

Antoine M., Gobert D., *"La directive européenne sur la signature électronique. Vers la sécurisation des transactions sur l'Internet ?"*, publié dans JTDE n° 68, Avril 2000.

Bates A J., *"One-Stop-Government, National Report - Ireland"*, draft, 1999.

Bellamy C., Brewer N., Petrie A., *"One-Stop-Government in England and Wales - National Report"*, Nottingham Trent University, 1999.

Bent S., Kernaghab K., Marson B., *"Les guichets uniques : innovations et bonnes pratiques"*, Réseau du service axé sur les citoyens , Centre canadien de gestion, Mars 1999.

Chambre des représentants de Belgique, *"Projet de loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification"*, Chambre des représentants de Belgique, 15 Février 2001.

Frankinet Ph., *"AdmiPRO, schéma LDAP"*, NSI s.a., 2000.

Frankinet Ph., *"AdmiPRO - schéma LDAP appliqué à PBFLow"*, NSI s.a., 2001.

Frankinet Ph., "AdmiPRO - Architecture Java", NSI s.a., 2001.

Frankinet Ph., *"AdmiPRO - Modules de signatures électroniques"*, NSI s.a., 2001.

Gallego R., Rosetti N., Ysa T., "COST PROGRAMME A14, Working Group 3 : Information and Communication Technologies and Public Administration, National Report on 'One-Stop-Government' (Spain)", Universitat Autònoma de Barcelona et Fundació Carles Pi i Sunyer, 1999.

Georgia State Research Fundation, *"Legal XML overview"*, Georgia State Research Fundation, 2000.

Gobert D., *"Belgique : projet de loi"*, publié dans Droit & Technologie, Février 2000.

Hagen M., Kubicek H., *"One-Stop-Governement in Europe : National Reports"*, Proceeding du Workshop international COST A14 tenu à Bremen (Allemagne) du 30 septembre au 2 octobre 1999.

Johner H., Brown L., Hinner F.-S., Reis W., Westman J., *"Understanding Ldap"*, International Technical Support Organization - IBM (www.redbooks.ibm.com), Juin 1998.

Journal officiel des Communautés européennes, *"Position commune (CE) n° 28/1999 arrêtée par le Conseil le 28 juin1999, en vue de l'adoption de la directive du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques"*, Journal officiel des Communautés européennes, 1999/C 243/02, Juin 1999.

Lobet-Maris C., *"Guichet unique, réalité plurielle. Résultats d'une enquête européenne"*, CITA, Janvier 2001.

Lobet-Maris C., van Bastelear B., avec la collaboration de De Vos A., *"COST Belgian National Report, One-Stop-Government in Belgium"*, *CITA-FUNDP*, second draft, Août 1999.

Marsocci P., Salza S., *"One-Stop-Government Projects in the Italian Public Administration"*, Università degli Studi di Roma "La Sapienza", 1999.

Michot O., *"Etude des techniques de signature numérique et mise en place dans le cadre du projet PBFlow"*, Mémoire de fin d'étude, Licence en informatique, Institut d'informatique, FUNDP, 2000.

Moniteur belge, *"Loi introduisant l'utilisation de moyens de télécommunication et de signature électronique dans la procédure judiciaire et extrajudiciaire"*, Lois, décrets, ordonnances et règlements, Ministère de la Justice, Moniteur belge, 22 Décembre 2000.

Netscape Communications Corporation, *"Netscape Directory Server 4.1, Deployment Guide"*, Netscape Communications Corporation,1999.

NSI s.a., *"AdmiPRO - Fiche Produit"*, NSI s.a., Mars 2001.

Poos W., *"AdmiPRO, Phase 1, Spécifications fonctionnelles et solutions techniques"*, NSI s.a., Octobre 1999.

Poos W., *"AdmiPRO, Phase 1, Architecture fonctionnelle et technique"*, NSI s.a., Juillet 2000.

Ramaekers J., *"Sécurité des systèmes informatiques"*, Institut d'informatique, FUNDP.

Ramaekers B., *"Sécurisation de PBFlow"*, 2000.

Robben F., *"Naar een elektronische identiteitskaart voor elke burger, als mogelijk drager van en elektronische handtekening"*, FEDICT (www.fedict.be), 2001.

Struyven D., *"La signature électronique : ses aspects juridiques"*, FEB, Mai 2001.

Sundsted T., *"JNDI Overview, Part I : An introduction to naming services"*, JavaWorld (www.javaworld.com), Janvier 2000.

Sundsted T., *"JNDI Overview, Part II : An introduction to directory services"*, JavaWorld (www.javaworld.com), Fevrier 2000.

Sundsted T., *"JNDI Overview, Part III : Advanced JNDI"*, JavaWorld (www.javaworld.com), Mars 2000.

Tyagi S., *"LDAP and JNDI: Together forever"*, JavaWorld (www.javaworld.com), Mars 2000.

Wang Y., *"LDAP makes peace between directory services"*, Netscape Enterprise Developer (www.ne-dev.com) , Janvier 1998.

Wery E., *"La signature électronique fait dorénavant partie du droit belge !"*, publié dans Droit & Technologie, Décembre 2000.

Wery E., *"La Chambre adopte le projet de loi relatif aux prestataire de service de certification"*, publié dans Droit & Technologie, Février 2001.

ANNEXES

A.1. Architecture technique d'AdmiPRO

A.1.1. Architecture générale

L'architecture technique[50] d'AdmiPro est de type trois tiers, c'est-à-dire q'un *client* s'adresse à un ensemble *d'objets transactionnels* encapsulant la logique administrative et s'adressant à un *serveur de gestion de données*. Cette architecture est illustrée de la façon suivante :

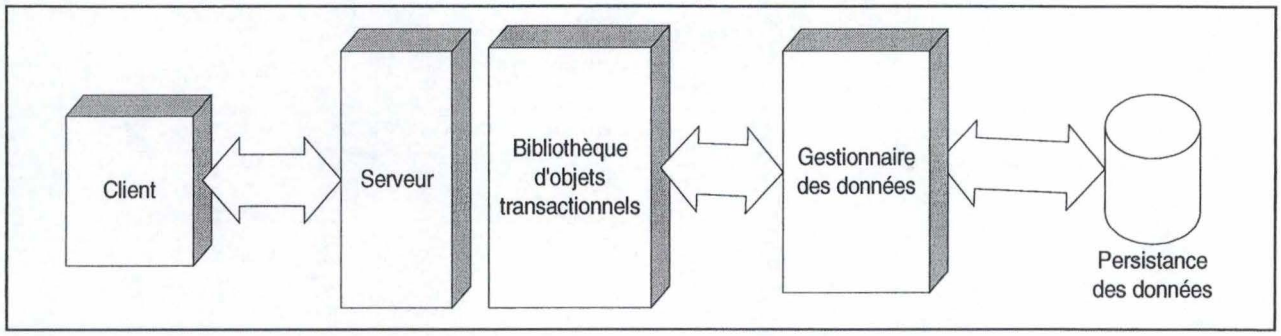

Figure 33. ANNEXE- ARCHITECTURE GENERALE D'ADMIPRO

Le client AdmiPro repose sur un ***navigateur standard***. Il s'agit d'un client léger utilisant le langage HTML (*Hyper Text Markup Language*) et le JavaScript. Un ***serveur Web*** auquel est associé un ***moteur Java*** compose le second bloc. Ces deux composants génèrent le portail administratif. Pour ce faire, ils intègrent la bibliothèque des objets transactionnels. La gestion des données est assurée par un ***SGBD*** (*Système de Gestion de Base de Données*).

A.1.2. Outils et bibliothèques d'objets

Le client, un navigateur standard, utilise le protocole HTTP (*HyperText Transfert Protocol*) pour échanger les informations avec l'environnement serveur. Le protocole HTTPS (*HTTP-Secure*) est utilisé pour l'authentification avec certificats électroniques.

L'environnement serveur repose sur un serveur Web et le langage Java. La bibliothèque d'objets transactionnels Java de AdmiPRO comprend les mécanismes d'authentification, la gestion du répertoire des organisations, la boîte de travail, l'audit et le suivi, la réalisation des tâches, la publication, la consultation et l'historique des dossiers et documents.

Le bureau de l'agent traitant est généré à partir de page JSP (*Java Server Page*) qui sont des pages dynamiques complétées par le serveur avant d'être envoyées au client. Les données insérées dans ces pages proviennent des objets transactionnels.

[50] Poos W., 1999

La figure ci-dessous reprend l'architecture technique Java d'AdmiPro phase I[51] :

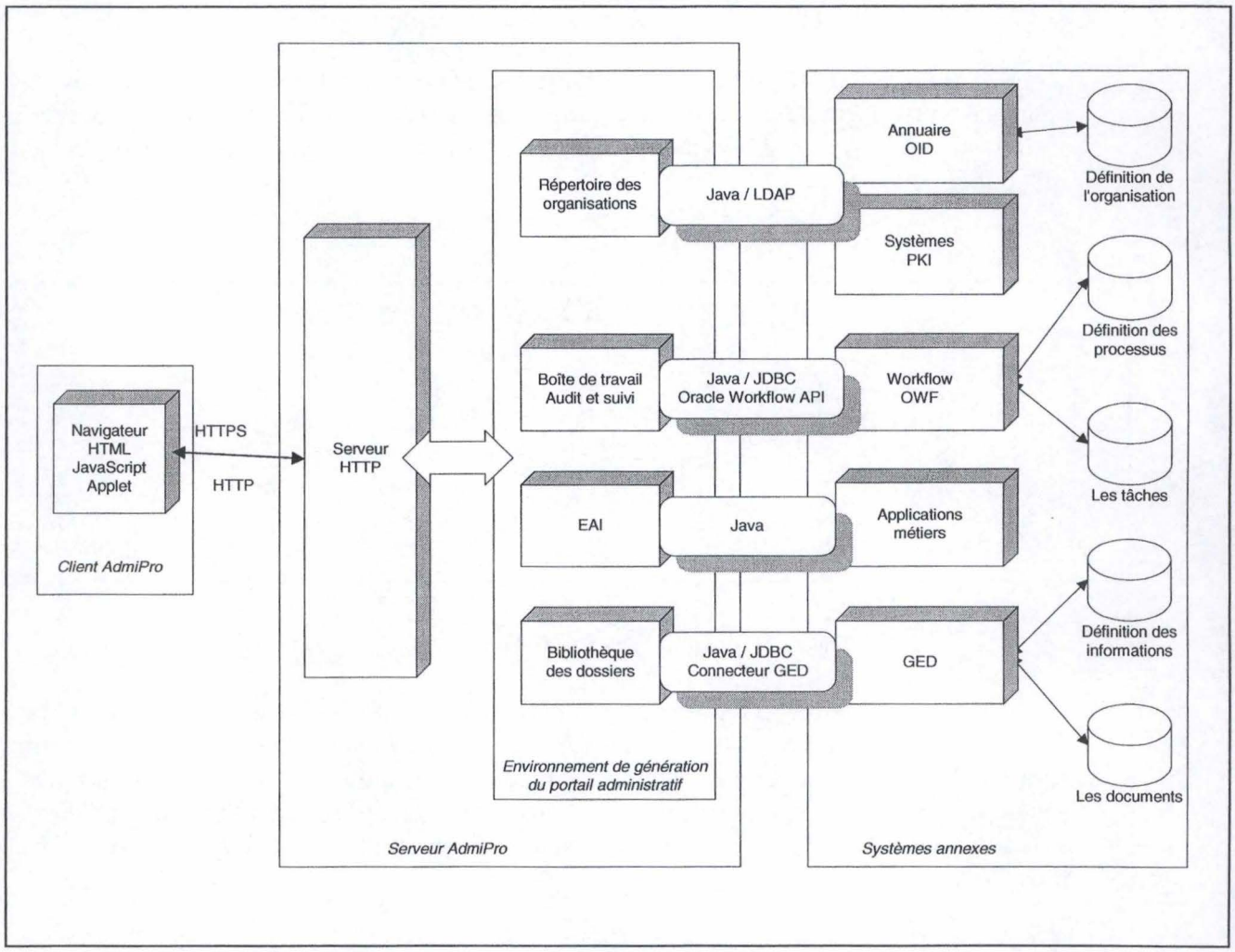

Figure 34. ANNEXE - ARCHITECTURE TECHNIQUE D'ADMIPRO

La ***définition de l'organisation*** et la ***consultation de l'annuaire organisationnel*** utilisent un annuaire électronique qui est Oracle Internet Directory. L'accès à l'annuaire est réalisé au travers d'objets écrits en Java qui utilise le protocole LDAP (*Lightweight Directory Access Protocol*). Un lien vers un système PKI (*Public Key Infrastructure*) est utilisé afin de valider les certificats électroniques des acteurs.

La ***définition d'information*** est réalisée au travers de modules Oracle Forms. Cette application permet de définir les différents types de documents, leur appartenance aux dossiers et à quel moment du flux administratif ils doivent être générés.

Le ***moteur d'exécution des procédures*** est assuré par Oracle Workflow qui possède aussi une interface graphique permettant de ***définir les processus***. La ***boîte de travail*** utilise d'ailleurs Oracle Workflow afin de présenter à l'utilisateur les différentes

[51] Frankinet Ph, 2001 (2)

tâches qui lui sont proposées ainsi que le parcourt effectué dans le flux administratif pour le dossier concerné.

La ***bibliothèque des dossiers*** regroupe les fonctionnalités de recherche et la librairie des opérateurs (dont la signature électronique). Une GED (*Gestion Electronique des Dossiers*) reprend l'ensemble des dossiers et documents. C'est le composant ***persistance*** d'AdmiPro. La GED AdmiPro est actuellement "propriétaire", c'est-à-dire qu'elle ne respecte pas les normes et interfaces pour ce type d'application. Elle est accessible en Java au travers de modules de connexion aux bases de données utilisant les JDBC (*Java DataBase Connectivity*). La ***recherche des dossiers et documents*** est réalisée au travers d'un outil nommé Oracle InterMedia. Cet outil supporte les recherches "full text", les synonymes et les approximations de langage.

Le module portant le nom de EAI (*Enterprise Application Interface*) sert à interfacer les ***applications métiers***. La réalisation de ces intégrations est faite au cas par cas, en utilisant des technologies comme "Advenced Queuing" et l'échange de messages XML (*Extensible Markup Language*).

A.2. Schémas entité-association du modèle organisationnel dans AdmiPRO

Le modèle des données définissant la structure organisationnelle est reprise dans un schéma entité-association[52].

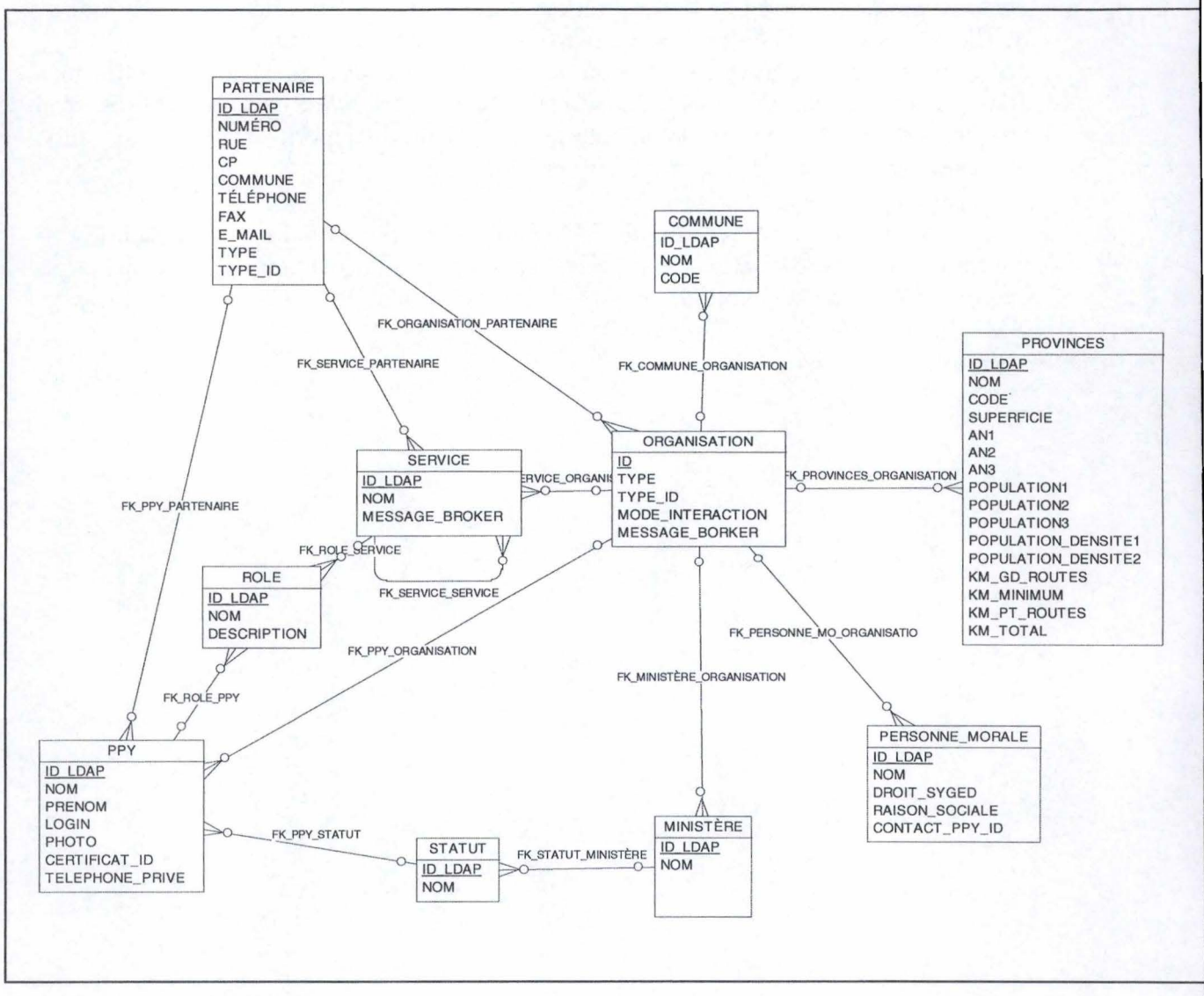

Figure 35. ANNEXE - MODELE DES DONNEES DE L'ORGANISATION DANS ADMIPRO

[52] Poos W., 2001.

A.3. LDIF : LDAP Data Interchange Format[53]

LDIF est un format d'échange utilisé par les annuaires électroniques. Il est particulièrement intéressant d'utiliser ce format lorsque de nombreuses opérations doivent être effectuées, comme par exemple l'ajout de plusieurs entrées ou la modification d'un certain nombre d'attributs.

A.3.1. Format LDIF

Une entrée de l'annuaire se représente comme une suite de ligne décrivant les propriétés de cette entrée. Prenons l'exemple d'une entrée standard en LDIF :

[<id>]
dn: <distinguished name>
objectclass: <object class>
objectclass: <object class>
...
<attribute type>[;language tag]:<attribute value>

Terme	Description
[<id>]	ID optionnel (nombre positif). Généré par défaut par les outils de l'annuaire.
dn: distinguished name	Le DN de l'entrée
objectclass: <object class>	Classe de l'entrée, qui détermine entre autres les attributs obligatoires ou optionnels de celle-ci.
<attribute type>	Type de l'attribut
language tag	Langue dans laquelle est exprimée la valeur de l'attribut. Le type d'attribut doit évidemment être du texte
<attribute value>	Valeur de l'attribut

Dans le cas particulier où la valeur de l'attribut est une valeur binaire, comme par exemple une image, la valeur est codée en Base64. Afin de noter cette valeur, le séparateur est doublé : <attribute type>[;language tag]*::*<attribute value>

Lorsqu'un attribut est multivalué, on spécifie une valeur par ligne. C'est aussi le cas pour les classes, car l'ensemble des classes de l'objet doit être présent et non pas seulement la classe la plus spécialisée.

[53] Johner H., Brown L., Hinner F.-S., Reis W., Westman J., 1998

A.3.2. Quelques exemples liés à AdmiPRO

une organisation

dn: o=Ville de Namur,c=be
telephonenumber: +3281246347
objectclass: partenaire
objectclass: top
objectclass: commune
objectclass: organization
postaladdress: 50 rue de Fer
postalcode: 5000 Namur
description: Administration Communale de la Ville de Namur
code_ins: 3
o: Ville de Namur
abreviation: vdn

un service

dn: ou=Urbanisme,o=Ville de Namur,c=be
objectclass: service
objectclass: organizationalUnit
objectclass: top
ou: Urbanisme

une personne

dn: cn=Gilbert Isabelle,ou=Administratif,ou=Urbanisme,o=Ville de Namur,c=be
mail: isabelle.gilbert@ville.namur.be
accesadmipro: true
objectclass: organizationalPerson
objectclass: top
objectclass: person
objectclass: inetOrgPerson
objectclass: ppy
description:: Q29udGFjdCBwb3VyIFBCRmxvdyDgIFZETg==
cn: Gilbert Isabelle
sn: gi

A.4. AdmiPRO - Modèles des données en format LDIF

La modification du schéma de base de l'annuaire se fait via le format d'échange LDIF. Une entrée particulière de l'annuaire permet de consulter et de modifier ce schéma. Le nom de cette entrée est obtenu en interrogeant la racine de l'annuaire électronique.

La mise en place de la représentation organisationnelle d'AdmiPRO ou d'AdmiPRO appliquée à PBFlow a nécessité la modification du schéma via l'ajout d'attributs et de classes.

A.4.1. Attributs AdmiPRO

 # Abréviation // Utilisé par l'objet "partenaire"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.1.7 NAME 'abreviation' DESC 'Abréviation' EQUALITY caseIgnoreMatch SUBSTRING caseIgnoreSubstringsMatch SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

 # URL Photo // Utilisé par l'objet "ppy" et dérivés
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.1.8 NAME 'URLPhoto' DESC 'URL de la photo de la personne physique' EQUALITY caseIgnoreMatch SUBSTRING caseIgnoreSubstringsMatch SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

 # AccèsAdmiPro // Utilisé par l'objet "ppy" et dérivés
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.1.9 NAME 'AccesAdmiPro' DESC 'Détermine si la personne a accès à Admipro ou non' EQUALITY caseIgnoreMatch SUBSTRING caseIgnoreSubstringsMatch SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

 # Forme Juridique // Utilisé par l'objet "personne morale"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.0.1 NAME 'forme_juridique' DESC 'Forme juridique d'une organisation' EQUALITY caseIgnoreMatch SUBSTRING caseIgnoreSubstringsMatch SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

 # Raison Sociale // Utilisé par l'objet "personne morale"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes

attributetypes: (1.0.0.0.0.0.2 NAME 'raison_sociale' DESC 'Raison sociale' EQUALITY caseIgnoreMatch SUBSTRING caseIgnoreSubstringsMatch SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

A.4.2. Classes AdmiPRO

 # Objet Partenaire // Super-Type
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: (1.0.0.0.0 NAME 'partenaire' DESC 'Partenaire' SUP organization MUST abreviation MAY mail)

 # Objet Role
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: (1.0.0.0.8 NAME 'role' DESC 'Role' SUP organizationalRole MAY mail)

 # Objet Service
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: (1.0.0.0.9 NAME 'service' DESC 'Service' SUP organizationalUnit MAY mail)

 # Objet PPY
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: (1.0.0.0.5 NAME 'ppy' DESC 'personne physique' SUP inetOrgPerson MUST AccesAdmiPro MAY URLPhoto)

 # Objet PMO
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: (1.0.0.0.3 NAME 'pmo' DESC 'Personne morale' SUP partenaire MUST (forme_juridique $ raison_sociale $ roleOccupant))

A.4.3. Attributs AdmiPRO appliqué à PBFLow

 # CodeIns // Utilisé par les objets "commune" et "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.0.0 NAME 'code_ins' DESC 'Code INS' EQUALITY caseIgnoreMatch SUBSTRING caseIgnoreSubstringsMatch SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

 # Superficie // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.0.3 NAME 'superficie' DESC 'Superficie' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.27')

 # An1 // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.0.4 NAME 'an1' DESC '1ère année' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.27')

 # An2 // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.0.5 NAME 'an2' DESC '2ème année' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.27')

 # An3 // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.0.6 NAME 'an3' DESC '3ème année' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.27')

 # Population1 // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.0.7 NAME 'population1' DESC 'Population durant an1' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.27')

 # Population2 // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.0.8 NAME 'population2' DESC 'Population durant an2' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.27')

 # Population3 // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.0.9 NAME 'population3' DESC 'Population durant 3' SYNTAX
'1.3.6.1.4.1.1466.115.121.1.27')

 # Densité Population1 // Utilisé par l'objet "province"

dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.1.0 NAME 'population_densite1' DESC 'Desité de population pour an1' SYNTAX '1.3.6.1.4.1.1466.115.121.1.27')

 # Densité Population2 // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.1.1 NAME 'population_densite2' DESC 'Desité de population pour an2' SYNTAX '1.3.6.1.4.1.1466.115.121.1.27')

 # Densité Population3 // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.1.2 NAME 'population_densite3' DESC 'Desité de population pour an3' SYNTAX '1.3.6.1.4.1.1466.115.121.1.27')

 # KM grand routes // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.1.3 NAME 'km_gd_routes' DESC 'KM de grand routes' SYNTAX '1.3.6.1.4.1.1466.115.121.1.27')

 # Minimum de KM // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.1.4 NAME 'km_minimum' DESC 'Minimum de KM' SYNTAX '1.3.6.1.4.1.1466.115.121.1.27')

 # KM petites routes // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.1.5 NAME 'km_pt_routes' DESC 'KM de petites routes' SYNTAX '1.3.6.1.4.1.1466.115.121.1.27')

 # KM au total // Utilisé par l'objet "province"
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.0.0.0.0.1.6 NAME 'km_total' DESC 'KM au total' SYNTAX '1.3.6.1.4.1.1466.115.121.1.27')

A.4.4. Classes AdmiPRO appliquée à PBFlow

 # Objet Commune
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: (1.0.0.0.1 NAME 'commune' DESC 'commune' SUP partenaire MUST code_ins)

 # Objet Ministère
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: (1.0.0.0.4 NAME 'ministere' DESC 'ministere' SUP partenaire)

 # Objet Province
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: (1.0.0.0.2 NAME 'province' DESC 'province' SUP partenaire MUST code_ins MAY (superficie $ an1 $ an2 $ an3 $ population1 $ population2 $ population3 $ population_densite1 $ population_densite2 $ population_densite3 $ km_gd_routes $ km_minimum $ km_pt_routes $ km_total))

 # Objet Architecte
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: (1.0.0.0.6 NAME 'architecte' DESC 'architecte' SUP ppy)

 # Objet Particulier
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: (1.0.0.0.7 NAME 'particulier' DESC 'un particulier' SUP inetOrgPerson)

A.5. Schéma entité-association du modèle des documents dans AdmiPRO

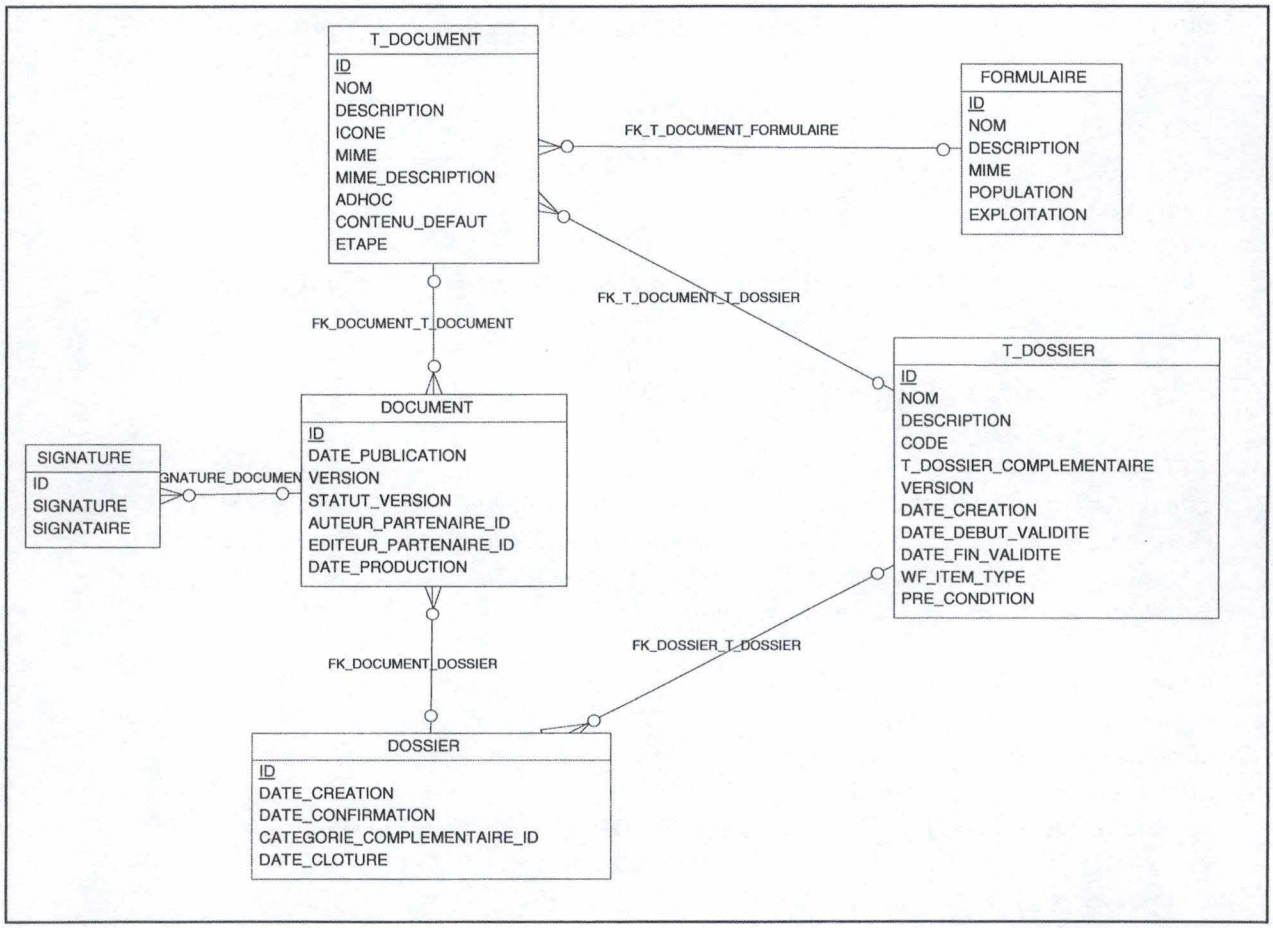

Figure 36. ANNEXE - MODELE DES DOCUMENTS DANS ADMIPRO

A.6. AdmiPRO - Architecture Java de la classe d'accès à LDAP

Cette libraire fournit les fonctionnalités les plus couramment utilisées lors de l'interrogation des annuaires électroniques. Citons entre autres :

- informations sur l'annuaire électronique
- lecture et manipulation du schéma de données
- recherche et liste
- manipulation des entrées

L'organisation des classes Java se fait selon la découpe suivante :

- les classes utilitaires
- les classes de définition de données
- les classes liées aux traitements

Les classes utilitaires comprennent les exceptions (les erreurs), les connexions et les contrôles étendus.

Classes utilitaires		
Classe	**Hérite de**	**Description**
LdapException	Java 1.2 / 1.3	Exception utilisée pour notifier une erreur
LdapConnectionException	LdapException	Exception utilisée pour notifier une erreur de connexion
LdapConnection	Java 1.2 / 1.3	Fournit le mécanisme de connexion à l'annuaire
LdapControls	Java 1.2 / 1.3	Fournit les diverses options de contrôles utilisées dans les recherches

Les classes de définition de données reprennent exclusivement les informations du modèle des données. Les données retournées par les classes de traitements sont en fait des objets Java standards.

Classes de définition de données		
Classe	**Hérite de**	**Description**
SchemaDefinition	Java 1.2 / 1.3	Définit les informations de base sur le schéma LDAP
AttributeDefinition	SchemaDefinition	Définit les informations sur les attributs
ClassDefinition	SchemaDefinition	Définit les informations sur les objets
MatchingRuleDefinition	SchemaDefinition	Définit les informations de comparaison et recherches
SyntaxDefinition	SchemaDefinition	Définit les syntaxes pour les attributs

Les classes liées aux traitements comprennent les recherches d'informations et les manipulations d'entrées.

Classes liées aux traitements		
Classe	**Hérite de**	**Description**
LdpaQuery	Java 1.2 / 1.3	Fournit un mécanisme générique d'interrogation de l'annuaire
LdapRootInformation	LdpaQuery	Permet d'obtenir des informations sur les propriétés d'adressage de l'annuaire
LdapSchemaInformation	LdpaQuery	Permet d'obtenir les informations relatives au modèle des données
LdapSearch	LdpaQuery	Permet de réaliser les recherches
LdapList	LdpaQuery	Permet de lister les entrées d'une branche de l'annuaire
LdapEntry	LdpaQuery	Permet de manipuler une entrée de l'annuaire

L'organisation de ces classes est représentée par le schéma ci-dessous :

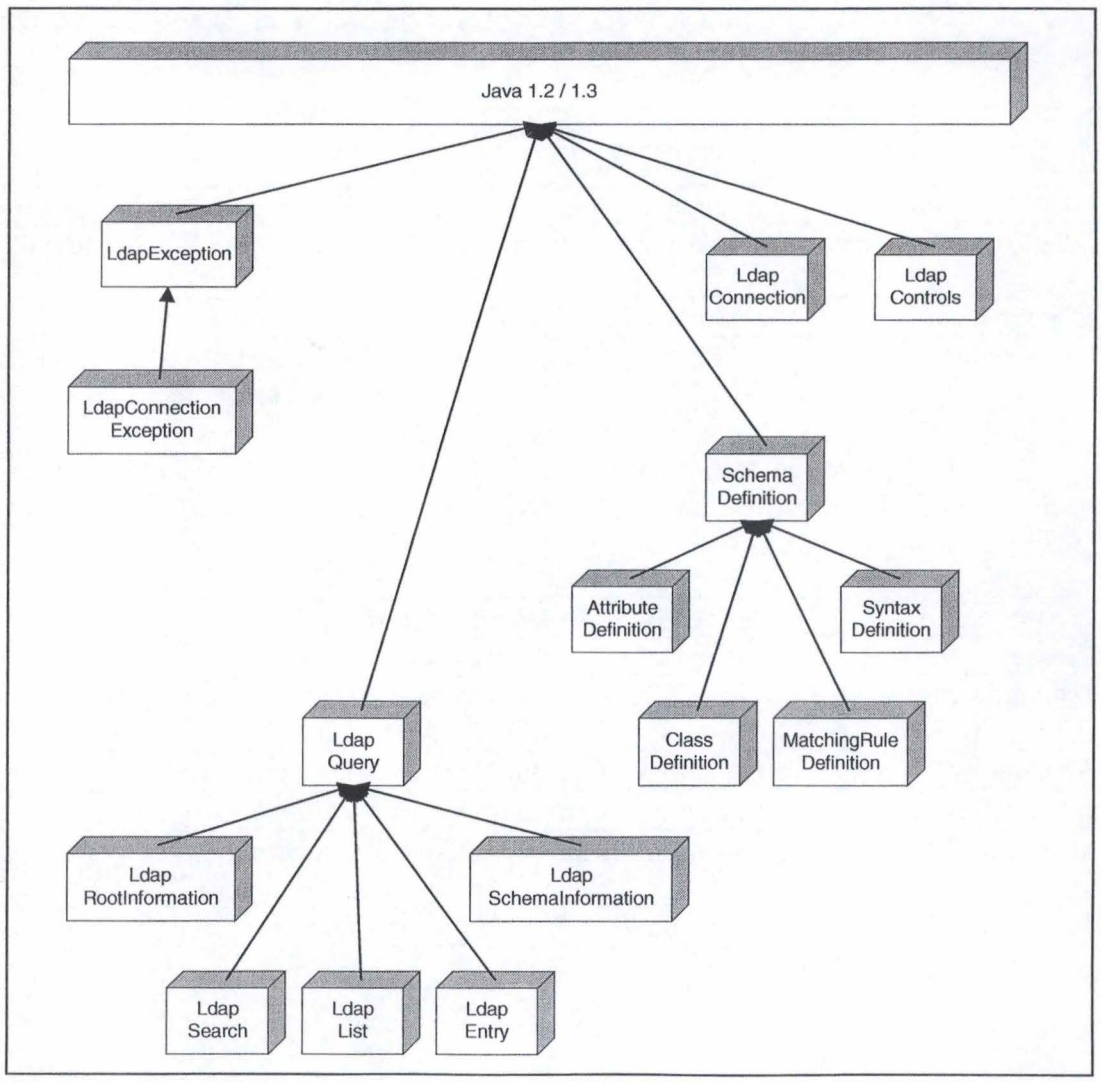

Figure 37. ANNEXE - ADMIPRO LDAP "BASE" : HERITAGE DES CLASSES JAVA

A.7. AdmiPRO - Architecture Java du connecteur JUnivers

Le connecteur JUnivers sert à transformer les demandes en requêtes compréhensibles pour LDAP et à retourner les données obtenues.

Le connecteur doit satisfaire aux exigences suivantes imposées par la librairie JUnivers :

- fournir les classes définissant les types de requêtes disponibles
- fournir les classes de filtres booléens permettant de définir les critères de recherches pour chaque type de requête
- fournir les classes de connexions et d'exécution des requêtes

Il faut remarquer que les requêtes sont organisées en deux groupes, à savoir les requêtes de recherche (de type « *AbstractQuery* ») et les requêtes de manipulation des entrées (de type « *AbstractOperation* »).

Les requêtes de lecture et les recherches sont reprises dans les classes suivantes :

Classes définissant les requêtes de lecture et recherche		
Classe	**Hérite de**	**Description**
AbstractQuery	Java 1.2 / 1.3	Fournit les mécanismes et les méthodes pour les lecture et les recherches
DefaultQuery	AbstractQuery	Fournit les méthodes de lecture pour tout type d'objet dont on spécifie la classe
EntryQuery	AbstractQuery	Fournit les méthodes pour les lectures d'une entrée
TreeQuery	AbstractQuery	Fournit les méthodes permettant de construire un arbre

Les requêtes de manipulation des entrées sont reprises dans les classes suivantes :

Classes définissant les requêtes de manipulation de données		
Classe	**Hérite de**	**Description**
AbstractOperation	Java 1.2 / 1.3	Fournit les mécanismes et les méthodes pour les manipulation des entrées
DefaultOperation	AbstractOperation	Fournit les méthodes de manipulations pour tout type d'objet dont on spécifie la classe
EntryOperation	AbstractOperation	Fournit les méthodes de manipulations d'une entrée

Les filtres booléens définissent les clauses de recherche, ces dernières étant transformées afin d'être comprise de LDAP. Il existe un filtre par type de requête.

Classes définissant les filtres booléens		
Classe	**Hérite de**	**Description**
LdapBooleanFilter	JUnivers	Définit les mécanismes afin de transformer les clauses booléennes en critères LDAP
DefaultBooleanFilter	LdapBooleanFilter	Filtre booléen pour les requêtes de type "défaut"
EntryBooleanFilter	LdapBooleanFilter	Filtre booléen pour les requêtes sur les entrées
TreeBooleanFilter	LdapBooleanFilter	Filtre booléen pour les requêtes de construction d'arbre

Enfin, le connecteur définit les mécanismes de connexion et d'exécution des requêtes.

Classes définissant la connexion et l'exécution des requêtes		
Classe	**Hérite de**	**Description**
LdapDataConnection	JUnivers	Définit le mécanisme de connexion
LdapDataQuery	JUnivers	Définit le mécanisme d'exécution des requêtes de type recherche ou lecture
LdapDataOperation	JUnivers	Définit le mécanisme d'exécution des requêtes manipulant les entrées

L'organisation de ces classes est représentée par le schéma ci-dessous :

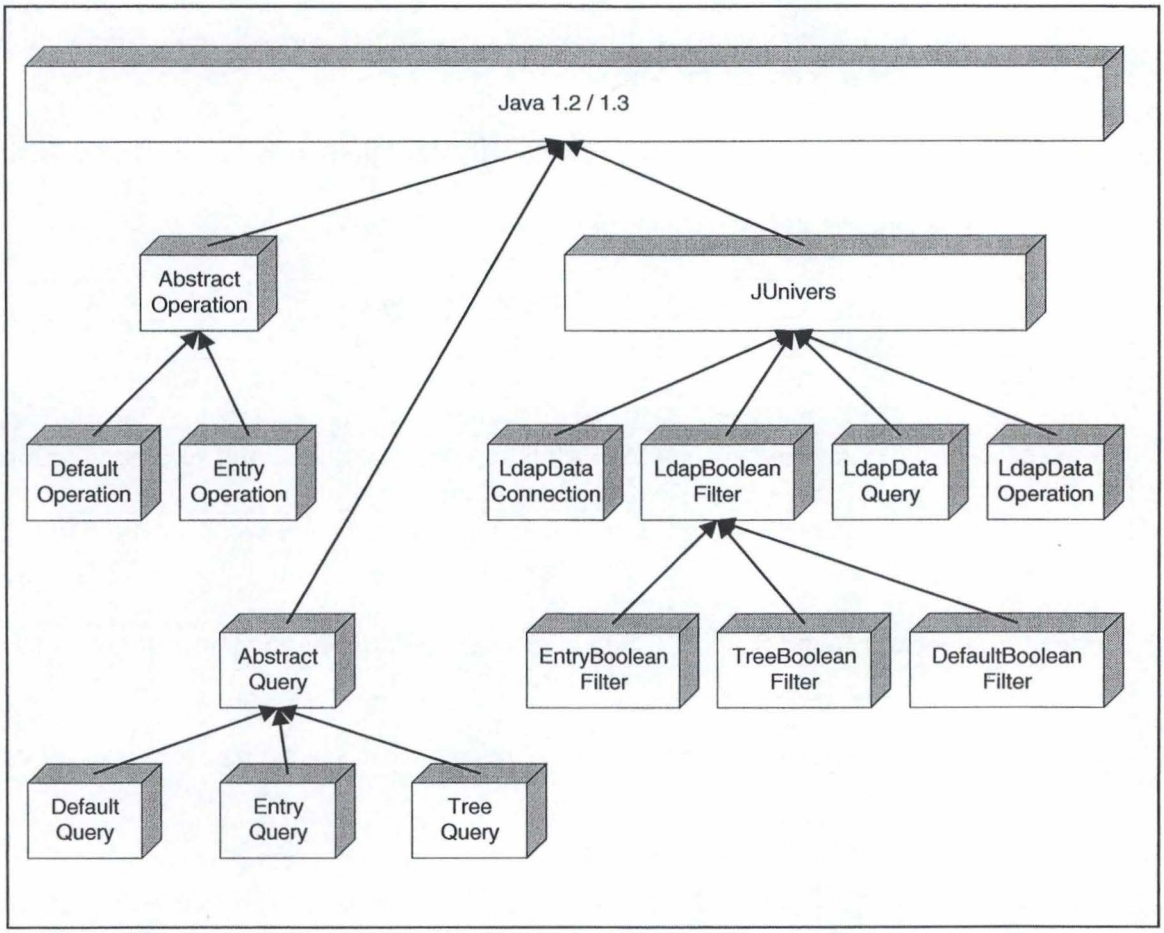

Figure 38. ANNEXE - ADMIPRO : CONNECTEUR JUNIVERS, HERITAGE DES CLASSES JAVA

A.8. AdmiPRO - Architecture Java de l'applet de signature

L'applet de signature a pour rôle de signer le document qui lui est présenté. Pour ce faire, elle demande au signataire d'encoder la passphrase permettant de lire la clé privée qui sera utilisée lors de la signature.

Une fois le document signé, elle expédie la signature au servlet de vérification.

Les classes reprises dans l'applet sont les suivantes :

Classes de l'applet		
Classe	**Hérite de**	**Description**
SignApplet	Java 1.1	Applet de signature à proprement parlé
Sign	Java 1.1	Permet de signer un document à l'aide d'une clé privée
Message	Java 1.1	Objet d'échange entre l'applet et le servlet. Contient entre autre la signature
AdmiProLayout	Java 1.1	Définit le layout (couleur, police, ...) AdmiPRO
PopUpError	Java 1.1	Element graphique permettant d'afficher un message d'erreur
PopUpPassphrase	Java 1.1	Element graphique permettant à l'utilisateur d'encoder sa passphrase

L'organisation de ces classes est représentée par le schéma ci-dessous :

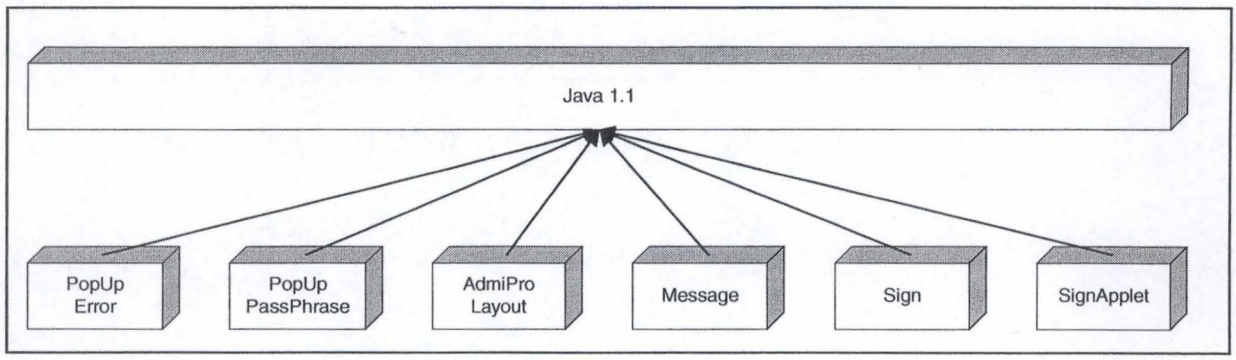

Figure 39. ANNEXE - ARCHITECTURE JAVA DE L'APPLET DE SIGNATURE DANS ADMIPRO

A.9. AdmiPRO - Architecture Java du module de vérification des signatures

Le module de vérification des signatures électroniques est implémenté au travers la mise en place d'un servlet. Ce servlet a pour rôle de vérifier les signatures émises par l'applet du poste client et si cette signature est vérifiée, l'insérer dans la gestion électronique des documents.

Les classes reprises dans le servlet sont les suivantes :

Classes de l'applet		
Classe	**Hérite de**	**Description**
UploadSignedStream	Java 1.2 / 1.3	Servlet utilisé pour la vérification et l'insertion dans le système de la signature électronique.
Verify	Java 1.2 / 1.3	Permet de vérifier un document.
Message	Java 1.2 / 1.3	Objet d'échange entre l'applet et le servlet. Contient entre autre la signature.

L'organisation de ces classes est représentée par le schéma ci-dessous :

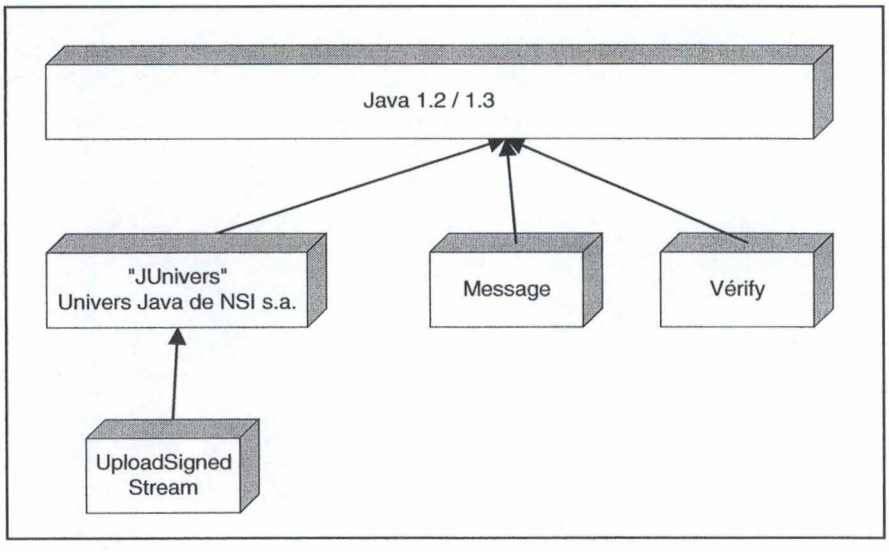

Figure 40. ANNEXE - ARCHITECTURE JAVA DU SERVLET DE VERIFICATION DANS ADMIPRO